Evidian

IAM for the extended enterprise

Trusted partner for your **Digital Journey**

Summary

04 'A major supermarket'

05 The changing face of identity and access

06 What we can do for Frank

06 Modeling the requirements for access rights

07 Making it easier to assign rights and monitor changes

07 Delegating responsibility to the business.

08 Ensuring that rights are complied with at all times.

08 Reusing existing infrastructures

08 The option to request an account and secure its activation

09 Smartphone authentication

09 No passwords to remember

10 Conclusion

10 Evidian IAM Suite

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

‘A major supermarket’

Frank, the CIO, and Cathy, the Group Marketing Director, one Monday morning at the coffee machine.

Frank: Hi Cathy.

Cathy: Hi Frank, how are you? You look worried.

Frank: Yes, on Friday, Ben, our CFO, called me because we have to put in place a system to identify who is connecting to the control system in every single store. We can’t just use generic store accounts any more.

Cathy: Well, it shouldn’t be that complicated, should it?

Frank: Are you kidding? With the vast number of staff changes we have in all our 80 stores across Europe, it’s impossible for me to know who has access to what. This is why we set up the generic accounts.

Cathy: So it’s really only the store manager who can know this. That’s right, isn’t it?

Frank: Exactly! Like we said, it’s only the managers and directors of a particular business area that are able to know who’s accessing what, and what rights they have.

Cathy: Why’s that? Don’t all the sales staff have the same rights?

Frank: Oh no, no, no... depending on their level of responsibility or the department where they work, the rights may be different. And for some applications, the store manager can give them direct access, but for the others the request has to be validated centrally and guess what...

Cathy: Go on...

Frank: To put it simply, it’s not always the same person in the central office who can validate the store manager’s request to give a member of the sales staff access to a particular application...

Cathy: Goodness, your job is starting to look pretty complicated, because now I come think about it, not all the stores have assigned managers.

Frank: There you have it! We’re going to have to allow sales staff to put in their own requests for access or event to self-register if they’re not yet defined on the system. You know, for payroll purposes, the person just has to be on the system before the last week of the month, but we have to prepare their working environment several days before their arrival, so they can start work right aways.

Cathy: And they have to be able to ‘activate’ their account themselves, very quickly, to ensure minimum security levels...

Frank: Well done Cathy!

Cathy: ...what’s more, you’re going to have to cope with new demands from your users. They’ll tell you they have to be able to log in from their phone, and without passwords. It’s easy to forget everything after a long weekend!

Frank: And there’s no question of changing anything on the Web site. It’s just been signed off by management and is accepted by all its users, internal as well as external.

Cathy: See you, and goof luck...

Frank, our CIO, has to ensure that his company complies with regulations. What’s more, he has to take into account the constant changes in new technology.
Now, let’s see how we can help him in this process, in terms of an IT and functional solution...

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 Frank is encountering in his supermarket business are the same that may be faced by an international financial institution, 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.

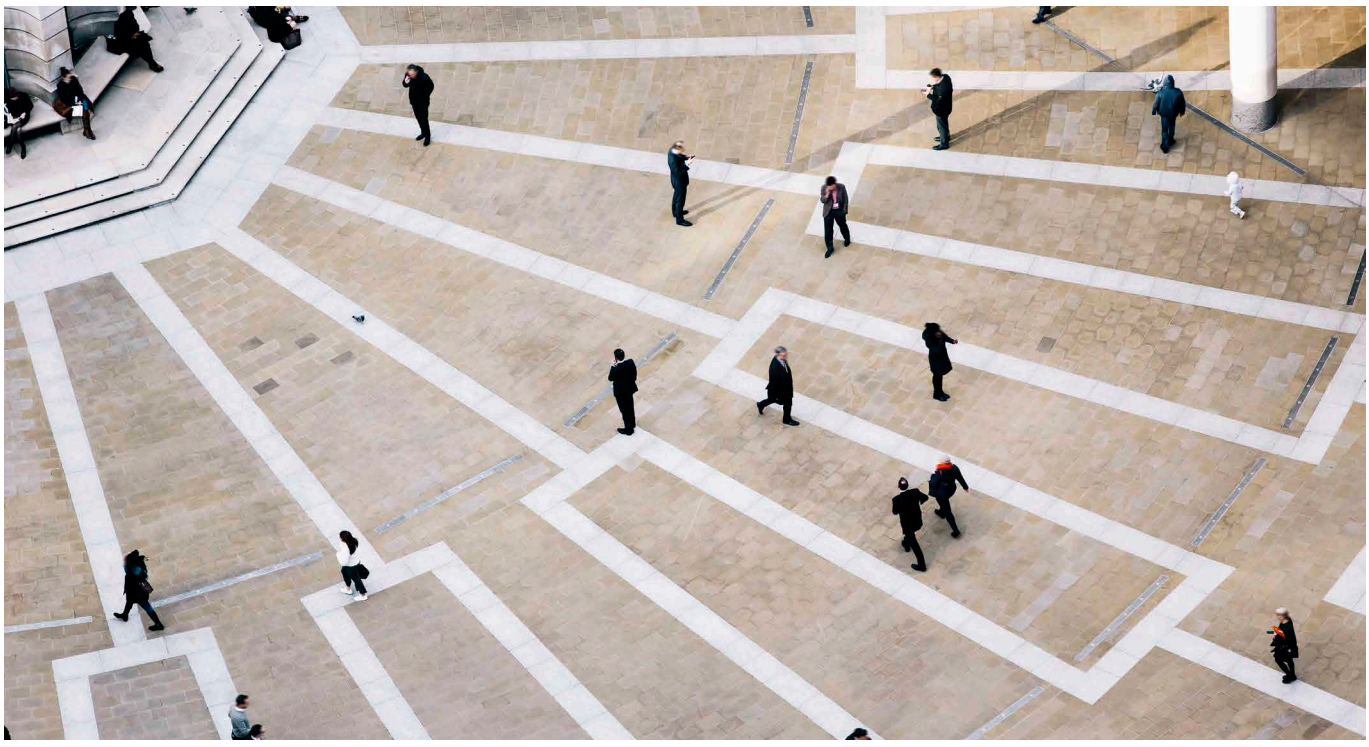
It is also important to be able to reuse current infrastructures, without having to modify existing elements such as the Web site.

Analyzing the discussion between Frank and Cathy, it's clear that the company needs to:

- Be able to assign unique accounts for each user, instead of using generic accounts, to ensure that access is both traceable and auditable,
- 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,
- 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. Of course, when they're making requests users need to be offered the right choice of applications appropriate to their job role, and requests need to be sent to the right people,
- Offer an 'account creation' request system to employees who have not yet been defined in the information system, to give them appropriately controlled access to it,
- 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,
- Allow users to authenticate themselves via their smartphone or tablet if they want to, with no need to remember a password in order to do their work, but without jeopardizing corporate security,
- And finally, to continue using the existing Web portal without it needing to be modified to provide the functionality described above.

Obviously, this not an exhaustive list of the features that Frank will require from the identity and access management solution that he 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 Frank, to help him solve his problem.



What we can do for Frank

The proposal to help Frank is based around the Evidian Identity and Access Management (IAM) Suite. The Evidian IAM Suite enables him to respond positively to the needs set out above, and to go 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 on the right.

Evidian IAM Suite facilitates the creation of an identity repository, including everyone entitled to access the information system from different identity sources. This repository includes not just employees, but also external people and partners as appropriate. The identity and access governance policy will apply to this identity repository.

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.

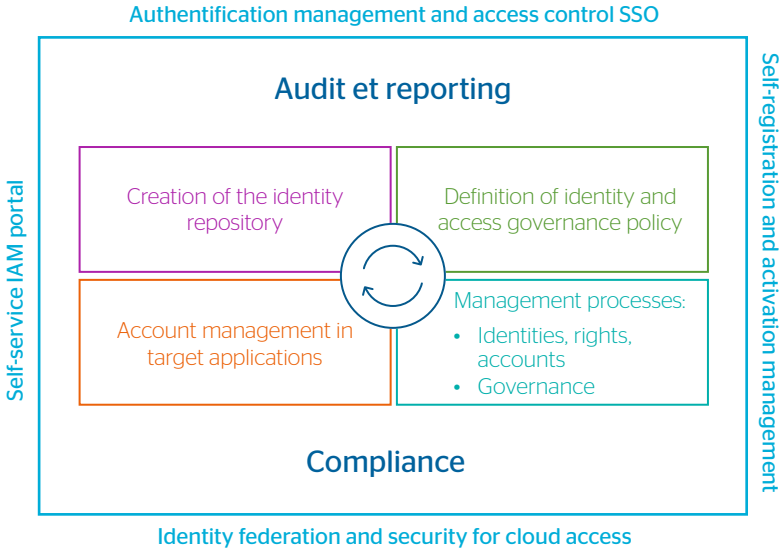
It also provides the functionality to:

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

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.

Evidian IAM Suite



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.

In the following sections we set out the benefits that Evidian IAM Suite will deliver for Frank and his company.

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.

For example, all department managers have a minimum of set of rights that they all share, as well as other rights depending on the department where they work (e.g. hi-fi, drinks...).

It's also possible, of course, to assign rights directly without going through role assignment: which is essential to deal with cases that cannot be modeled or exceptions to the rule.

The model also encompasses the concepts of organizational and hierarchical inclusion and exclusion, and the rules governing segregation of duties. The aim of these concepts is, on the one hand to facilitate the task of assigning the rights associated with a role and how they are managed, and on the other to 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'. Then you would indicate in the rights request process, that any request must be validated by a person with 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. By applying this context to the right to 'validate an access rights request', only requests for access rights from people in my team role, or store XX or external organizations will be sent to me.

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, to limit the information displayed in the white-pages directory, or to 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's also possible to define exceptions. For example, everyone working in store XX 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 stores operative who becomes warehouse manager 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 stores operative and the warehouse manager jobs 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's 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's much closer to the 'field', no matter where that is located.

What we can do for Frank

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.

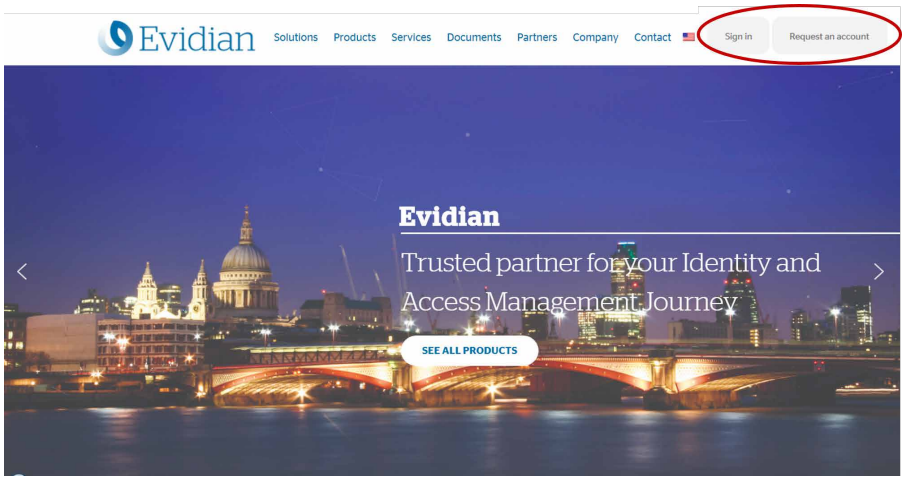
Functions such as reconciliation, which allow you to detect discrepancies between what has been defined as the rights an employee must have and the rights they have in reality. Corrective actions are then proposed, to allow the company to respond and close the gap.

Reusing existing infrastructures

Evidian IAM Suite can be integrated into existing environments with no need for modifications[1].

Frank talked about the fact that a new Web site had just been built, and said it was out of the question to modify it so as to incorporate the new features being requested. This is entirely possible with Evidian IAM Suite.

For example, the picture on the right shows the Evidian Web site is secured using IAM Suite, which provides authentication (shown in red). 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

Evidian IAM Suite allows users to request an access account.

In this current example, the person may indicate the store where she works, her job and email address, for example. Using this data, the mechanisms shown above help to ensure that applications are sent 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 he will use in the future to connect to the information system.

Once the account has been activated, the person can securely access authorized applications.

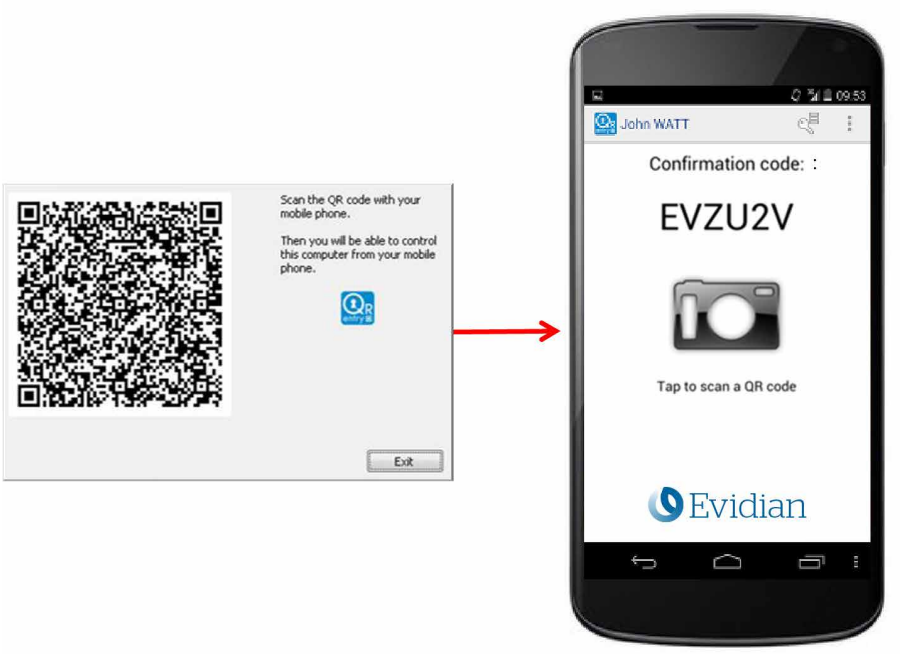
[1] "attention is nevertheless drawn to the fact that the technical environment in which Evidian software products may be installed must meet the technical prerequisites indicated in the product documentation."

Smartphone authentication

Evidian IAM Suite allows an employee to authenticate him/herself using a QR code via their smartphone. To do this, the employee needs to 'register' his/her smartphone with the business. This 'registration' is done through IAM Suite by the employee him/herself, with no need for the IT Department to get involved.

IAM Suite can authenticate users using other methods such as:

- User ID and password,
- The virtual keyboard. This 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.
- Social login (LinkedIn, Twitter...)



No passwords 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.

So if we take the case of an employee who uses his smartphone to authenticate himself on the company portal, Evidian IAM Suite allows Frank to announce that he has established a secure solution with no passwords to remember.

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

Conclusion

By implementing Evidian IAM Suite, Frank will deliver an identity and access management solution to his company that will enable it, among other things, 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,
- Provide simple and secure access without any passwords 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 Frank to meet his company's demands.

Evidian IAM Suite

Our IAM solution is recognized by customers and analysts for its completeness. The Evidian IAM Suite offers the following components to make a fully integrated solution:

Evidian Identity & Access Manager
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
is designed to manage access federation to Web applications, secure remote access for mobile users and replace all user passwords with a single and strong authentication method.

Evidian Enterprise SSO
facilitates access to enterprise and personal applications from workstations, mobile devices and smartphone and 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, failover, file replication and load balancing to applications.

For more information, visit our Web site: **www.evidian.com**

* General Data Protection Regulation

A prerequisite for GDPR*

Identity and Access Governance is one element among a range of technical counter-measures to mitigate risks related to data protection. In addition to its audit and certification campaign features, Evidian IGA takes into account the requirements for Users' Rights. The dedicated personal data reports and self-service functionalities allow users to exercise their rights freely and enable GDPR compliant processes.

About Evidian

Evidian is the Identity and Access Management (IAM) software suite of Eviden.

Evidian IAM is the European leader in identity and access management with a presence which is growing rapidly beyond Europe, particularly in Japan and the US.

More than 5,000,000 users in more than 900 organizations throughout the world connect to their companies every day and manage their access rights with Evidian identity and access management solutions.

CT_J1269_180803_RY_B_IAMFORTHEEX