

# IDENTITY AND ACCESS MANAGEMENT: DEFINING A PROCEDURE AND ORGANIZATION MODEL WHICH, SUPPORTED BY THE INFRASTRUCTURE, IS ABLE TO CREATE, MANAGE AND USE DIGITAL IDENTITIES ACCORDING TO BUSINESS POLICIES AND REGULATIONS

Within a context characterized by a multitude of business reorganizations, a growing need to comply with laws, regulations and standards as well as by an increasingly complex technological environment, it is vital to maintain the control and administration of users' credentials, as well as access control by identifying and managing the so called "Digital Identity". The IAM system provides a series of services to support the management of Digital Identities.

To develop an Identity and Access Management project, it is necessary to adopt a methodological approach enabling to start from the analysis of the current situation, of regulatory requirements and security objectives, in order to set up a solution implementation strategy. Spike Reply develops Identity and Access Management projects using a proprietary methodology able to adapt to the Client's specific requirements and checked using the best-of-breed technology solutions available on the market.

## THE THEME AREA

The economic crisis is intensifying two well known phenomena: business reorganizations on the one side and a generalized feeling of dissatisfaction among employees or those who are turned out of the Company on the other. In order to keep this phenomenon under control and reduce its impact, the main Organizations continuously increase controls on law, regulations and standard compliance. Moreover, such scenario is also characterized by an increasingly complex technological environment which renders even more difficult the attempt to keep control over the whole situation.

Having said that, it is fundamental to maintain the control and administration over user's credentials , as well as access control, by identifying and managing the so called "Digital Identity". As a matter of fact, since the traditional implementation of a company security policy consists in the setting up of a network of authorizations given to specific users, the process according to which their identities are managed (creation, change, cancellation) and the specific authorizations are granted, is the basis, often overlooked, on which the security of the whole information system is built.

Within the previously described scenario, the issue of users management is further complicated, in virtue of the multitude of technological specificities of each company: a heterogeneous set of applications and working environments which interact a little or not at all, with one-another, each having its own authentication system and its own identity repository.

This situation entails:

- The need of users to authenticate with different credential for each application, thus having to remember numerous username and password combinations ;
- A workload increase for IT personnel, due to the need to apply different tools, policies and procedures for the management of each application users;
- A workload increase for the Help Desk having to support users who forget their access credentials of the correct policy implementation;
- A decrease in the general security level since the whole architecture is generally simplified as much as possible and aligned with the service having the lowest security level;
- The impossibility to comply with regulatory requirements: often, the complexity of such processes does not allow the compliance with Business regulatory requirements or with possible requirements by external government bodies.

## THE SOLUTION

The term “Identity and Access Management” indicates the whole process (implementation of adequate policies and use of technological tools) required to manage information concerning users’ identity and control their access to the company’s resources.

From a technological point of view, the term IAM traditionally include the Centralized Repositories where the Digital Identities are stored (Enterprise Directory Services) and the Technological Services which allow their Management. The objectives of the IAM solution are the following: increase the productivity and user-friendliness of the IT system for end users, increase the general level of security, thus curbing costs related to the management of users and their identities, features and credentials. Basically, the aim is to create a tool able to support the process which decides which persons have access to what resources, the authorization allocation, authorization changes or revocations whenever necessary as well as the management of the whole process and the monitoring of all activities, in full compliance with the security business policies.

Therefore, IAM is not a turnkey solution but rather a business strategy allowing the implementation of a set of solutions involving the whole organization: IAM is a set of technologies and business processes. For this reason, there is not one single approach to the Identity and Access Management issues, since the implementation strategy of each organization must reflect its specific business requirements and its related technological context.

**THE TECHNOLOGICAL MODEL.** The technological model supporting IAM processes is divided into four main pillars: Identity Management Services, User Provisioning Services, Access Management Services and Single Sign-On Services. These pillars are “fed” by Policy Management and Audit functions and must be accompanied by High Availability, Scalability and Distribution Services. They include modular technical solutions, which may be implemented as single components or part of complete suites.



The components are:

- Identity Management
- ID Synchronization
- User Provisioning
- Workflow
- User Self Service
- Audit and Reporting
- Compliance and Role Management
- Enterprise Single Sign-On
- Strong Authentication
- Web Access Management
- Federation Services.

## THE IAM PROJECT

Spike Reply supports companies /organizations during all the phases of the “IAM Project” which may consist in the following activities:

**THE PROFILE MODEL.** The first fundamental step in the development and implementation process of a IAM strategy is to understand which are the main business requirements, by identifying key processes, critical applications and all the information necessary to comply with the business objectives. During this analysis phase the business organization is required to define which users must access specific resources and with what security level. For many companies, this analysis phase may be an excellent opportunity to review internal policies and processes which may not be so effective. The outcome of this phase is the setting up of a profile model and the mapping of administration processes.

**AUTHORIZATION AND POLICY MANAGEMENT.** At the core of each IAM strategy is the need to define a series of authorizations and security policies and ensure real-time implementation. Many organizations have found out that the best way to ensure an effective monitoring of authorizations is that of assigning access authorizations to resources on the basis of the user’s role within the organization; therefore, a shift towards a policy management based on functional roles becomes the key element of this project phase. This phase also includes Compliance Management, which aims at verifying the identified profile model, before its set up.

**USER PROVISIONING AND WORKFLOW.** The set of administration operations leading to the setting up of users accounts and the assignment of access rights on the bases of their role, is called User Provisioning; an effective IAM solution introduces a system for the centralized management of the whole administration process. The Workflow Component supports this tool, since it allows the automation of the provisioning process by sending the notifications required for the completion of the whole process to the relevant systems and also to individuals.

**USERS AUTHENTICATION.** Authentication is the process that verifies a user's identity in order to correctly allow or deny access to shared and protected resources. The authentication techniques may vary considerably from a simple login with username and password to more complex and strongest mechanisms such as tokens, public key digital certificates and biometric systems.

Therefore, an IAM solution must be independent from the authentication mechanisms used, in order to adapt to each specific technological situation. Moreover, in an organization whose scenario is the one originally described above, the user often has to access many applications, whether web-based or client-server, which require the use of numerous different credentials. For this reason, another key element of an efficient IAM strategy is the implementation of a Single Sign-On solution: this allows, on the one hand, to simplify users' work and on the other hand to reduce the administrative workload of the IT personnel, as well as of the Help Desk support.

In virtue of what has been said above, with regards to resources, time and costs necessary to create an IAM solution, it may be useful to highlight that such solution may be developed in different phases: the implementation strategy must always be based on the business priorities of the organization, starting, among the above listed activities, from the one which the company considers a priority; here are some examples:

- The introduction of a new application which has to be distributed to a large number of users (with relating authentication credentials) necessarily shifts the attention towards a user provisioning solution, allowing a more efficient management of administrative processes;
- an organization working mainly on e-business activities may introduce an IAM solution focusing more on the application rather than on the organizational aspects;
- the need to streamline users' work, complicated by the numerous access credentials required for different applications, leads to focus mainly on a Single Sign On solution.

## THE REPLY VALUE

The success of an IAM solution does not depend only on the involvement of IT personnel, but on the support and commitment of the whole business organization.

Spike Reply, thanks to the deep knowledge and skills available within the Reply Group, develops Identity and Access Management projects using a proprietary methodology able to adapt to the Client's specific requirements and checked using the best-of-breed technology solutions available on the market. It is therefore an ideal partner, well knowledgeable both with regards to the technological aspects, on the choice of solutions which best suite the main Client's business, and with regards to the organizational aspects, on the analysis of the approach methodology to Identity and Access Management issues and the reviewing of the resulting organizational processes.

With regards to IAM, Reply is engaged in international projects in complex sectors like Finance and Industry.

Starting from its extensive experience, the deep knowledge of technologies, operators, reference standards and laws, and performing a thorough check-up of the implemented counter-measures, of operational and organizational procedures, of systems configurations, of applications and of networks, Spike Reply is able to help Clients build the most efficient "shield" against any type of threat and providing best protection during all the intervention phases.

Specifically, Spike Reply is able to provide:

**Consultancy** (Security Planning, Risk Analysis and Management, Legal Compliance, Policy and Procedures, Security and Information System Verification, Security Consolidation)

**ICT Solution Planning** (Feasibility studies, Project assessment, Software selection, Project selection)

**ICT Solution Development** (Turnkey solutions, Management and Maintenance, Monitoring, Help Desk, Test)

**Training** (Business Security Awareness, ICT Training)

When carrying out its activities, Spike Reply avails itself of all the resources shared within the Reply Group and of relationships established within a network of partner companies providing mainly technology products or consultancy services.



Within the Reply Spa Group, Spike Reply is the company specialized in the field of Security and Personal Data Protection.

Spike Reply developed a comprehensive, integrated and consistent offer, in order to tackle any aspect of risks associated to an information system: from detection of threats and vulnerabilities, to the definition, planning and implementation of technological, legal, organizational, insurance or risk retention counter-measures. The Spike Reply mission is to allow its customers to perform their business in a secure environment, thus supporting them during the development and implementation of adequate strategies and solutions, for an effective management of Information Security.

Spike Reply  
[www.reply.eu](http://www.reply.eu)