



Generali Group Switzerland

Role-based identity management

www.siemens.com

SIEMENS

Role-based identity management

Assicurazioni Generali, Italy's leading insurance company, is the third largest European insurer in the life sector and controls 626 companies worldwide, among them Generali Group Switzerland. The Swiss firm chose Siemens to supply an Identity and Access Management solution to automate rights management across a range of diverse systems.

A series of mergers and acquisitions has brought a number of formerly independent Swiss insurance companies under one roof, resulting in rapid growth in the number of IT users requiring access to a broad range of services, data and applications running on a variety of platforms across Generali Group Switzerland. Resource provisioning is still performed manually using printed paper forms to assign each user a set of access rights to a specific configuration of systems and resources.

Manual rights assignment has worked well enough in the past, but with today's increasingly complex IT environments, it has become costly, time-consuming and subject to frequent errors. The mission of Enter Jürgen Lorek, an IT professional at Fortuna Life Insurance, one of the companies that now forms a major component of Generali Group Switzerland: Find a solution to automate rights management.

The project

For several years, Jürgen Lorek studied on his own time, adding complementary business and financial analysis skills to his professional IT expertise. Seeking a means to frame the resource provisioning issue in terms that will facilitate dialogue with non-IT colleagues and external solution providers, he has chosen an object-oriented analysis and design tool known as UML (Unified Modeling Language) to analyze and model Generali Group Switzerland in terms of its organizational structure and business processes.

The model proved effective, as Mr. Lorek says: "The UML model was a real milestone. It was clear that if we could find a product capable of implementing it, we would have a solution."

Roles

The principal objective of Mr. Lorek's project proposal, which referenced an emerging standard known as Role-Based Access Control (RBAC), was to replace the labor-intensive, system-specific assignment of user rights and permissions then in place at Generali by "a strategic ... centrally administered directory service (role concept) based on standards (X.500, LDAP) ..."

When he subsequently transferred from IT to Generali's Internal Audit division, Mr. Lorek took the project with him. Researching potential suppliers, he frequently saw the name 'Siemens' and soon discovered that the DirX metadirectory solutions suite was built around a role-based approach to identity and access management. "There were a number of white papers on the Siemens web site that talked about DirX. I drank them up like a good wine – the descriptions, the structures, the semantics, the language, the importance of objects, the descriptions, relationships – it all fit one-to-one. I haven't seen anything else that even comes close." As a result, Jürgen Lorek decided to contact Siemens.

The choice of a partner

Over the next several weeks, Siemens representatives from Germany and Switzerland met with the Generali team. Discussions focused on the role-management functionality of DirX; a turning point in the decision-making came when Jürgen Lorek presented his UML model to Siemens experts. The ensuing discussion proved convincing, and Siemens then invited Mr. Lorek to visit Munich for a closer look at DirX and discussions focused on the integration of Generali's legacy applications into the projected solution. Generali management then gave the project the green light.



Putting theory to work

Generali Group Switzerland's Legal Protection division, which offers legal costs insurance, was targeted for the initial implementation. The users required differentiated access to diverse resources and services: sales administration, contract management, and damage-assessment systems (all running under Oracle), and Microsoft ADS/Exchange.

A great deal of preparatory work had gone into the description of specific job functions and their definition in terms of roles, and a key requirement was to enable HR personnel to perform a "user-to-role" assignment for each employee. Once the name, address, salary, contract start, effective date of entry, etc. was registered, the HR manager was to assign a role corresponding to a specific job. At that point, the automatic procedures would take over: the entire user-to-role assignment would be read from the HR database and passed back to DirX, where the corresponding assignment of access rights was to take place.

Effective Integration

Simple enough in theory, but making it possible was a challenge. The objective was to achieve flawless synchronization between the metadirectory and the HR management system. Fortunately, Siemens had foreseen the possibility that customer-specific extensions of DirX might be necessary for effective integration in legacy environments, and Generali took advantage of this capability.

Nevertheless, Mr. Lorek says, "We had some fairly serious problems. We discovered some errors that required the direct intervention of the product developers in Germany." The Siemens developers were able to correct the errors quickly, however, and the difficulties were overcome.

Synchronization between the directory and the Generali application systems was equally critical. Once the role-based rights configurations had been integrated in the DirX metadirectory, they had to be mapped back into the different application systems and resources accurately. Mr. Lorek emphasized the "make or break" character of the task: "Our core business is built on the Oracle platform and is structured very similarly across the different applications, so this backwards compatibility with the current database applications in production was absolutely critical."

From complex to simple

And the result? The short answer – no problem – hardly does justice to the effort. Today, however, when a person is hired and assigned a role, or when role assignments change, all that is required from Generali's HR manager is to check a box on screen. DirX reads the status of all user-to-role assignments – enabled, added or deleted – and the result is automatically synchronized with the entire legacy system. As Jürgen Lorek notes, "The whole complexity of the paper-based, manual process in place prior to the project has been reduced to a single mouse-click."

A success story

The DirX-based Identity Management solution has been in production in the Legal Protection division since June of 2004. Looking back, Mr. Lorek commented, "We underestimated the amount of work involved, but we also underestimated the impact our success would have on the organization." As the solution is rolled out to the rest of Generali Group Switzerland, he will be able to count on additional resources.

In the meantime, integration of remaining non-core applications continues, and the benefits have begun to make themselves felt in terms of significantly lower administration costs; near-perfect accuracy in terms of moves, adds and changes; and greater confidence in the security of the IT environment and the company's ability to satisfy evolving regulatory requirements.

Identity and Access Management – a recommendation

Today, Jürgen Lorek is happy to recommend the Siemens solution and Siemens as a partner – it isn't hard to justify the investment when you look at the results. "Under the previous manual system it could easily take three or four hours and involve several different people in HR or IT administration to correct an error in rights assignment – that costs something. And if you think about the potential damage from misuse of obsolete or erroneous access rights ... the risks are obvious."

The Siemens solution has improved the security of Generali Group Switzerland systems and thus significantly reduced the risk of misuse and potential damage to the business.



Interview with Jürgen Lorek: A business point of view

Jürgen Lorek brings a solid background in Information Technology, business and finance to his current position with Generali Group Switzerland. He assumed responsibility for the project while working in IT, and took it with him when he transferred into the Group's Internal Audit division in 2002. His remarks below are excerpted from a conversation on the subject of Identity and Access Management at Generali Group Switzerland.

Q: Although you have a background as an IT professional, you also brought a business point of view to the challenge of resource provisioning. Can you give us a little more detail?

Jürgen Lorek: I was lucky in the sense that I could take on both the IT and the business analysis and bring them together in a form of interdisciplinary thinking. We began with classical organizational theory and looked at Generali's business in terms of how it was organized and in terms of business processes, as an operational organization. We evaluated all of the resources available in the company under these two points of view.

Although functions often cross departmental divisions, it's very difficult to change the way people traditionally think and work, so we're proceeding on a two-track path. As far as provisioning is concerned, we've introduced an operational structure. We have DirX set up to map functional responsibilities in terms of roles and corresponding privileges. We've modeled everything that a person does within the enterprise, the day-to-day business in a functional organization as well as project-oriented business, and together that provides the summa summarum of all rights and privileges for that person.

Q: What sort of impact did this approach have on the project?

Jürgen Lorek: I think it's one of the main reasons the project has been successful – the fact that we were able to convince management to look at it as a business issue rather than as a purely technical challenge. It was a business and organizational challenge that could be resolved using IT tools.

Role-based provisioning

Role-based provisioning is based on the Role-Based Access Control (RBAC) standard developed by the National Institute of Standards and Technology (NIST).

Siemens DirX solution deployed at Generali Group Switzerland enables cross-platform provisioning at a level closely mirroring the organizational structure of the enterprise. The definition of roles, role hierarchies, relationships, and constraints reflects the levels of responsibility and specific operations to be executed by persons in particular jobs. Each role is assigned one or more permissions containing bundles of access rights, and each employee is assigned one or more roles.

The DirX solution enables access rights to be granted, refused, withdrawn and monitored dynamically, independently of the platforms and applications used. Once a role-based framework has been put in place for an organization, the principal administrative actions are the user-to-role (user-to-job) assignments.

Siemens Enterprise Communications GmbH & Co. KG is one of the world's leading suppliers of Unified Communications technologies. The company's unique Open Communications approach to providing software, solutions and services for enterprises of all sizes enables business processes to be more productive, faster and more secure – with any device, network or information technology infrastructure. The company is a wholly owned subsidiary of Siemens AG with global headquarters in Munich.

With our Open Communications concept, we offer our customers cutting-edge solutions and services that are based on open standards and integrate seamlessly in their existing infrastructures and business processes.

In doing so, we are continuing to pursue our goal of realizing universal communications – across network and media boundaries and with a uniform user experience. We deliver added value to our customers by protecting their investments and enabling a phased implementation of our solutions that are tailored to their needs.

Open Communications from Siemens Enterprise Communications – award-winning solutions for everyone.

Siemens IT Solutions and Services – the Siemens IT powerhouse – embodies the comprehensive IT expertise of Siemens. We pool the IT know-how gathered by the company over the course of decades in the area of software development, services and solutions. We have no rivals on the market in providing industry and business process expertise from a single source. In fiscal year 2007 Siemens IT Solutions and Services employed some 43,000 people around the world and generated sales of around € 5.4 billion.

The business unit Identity Management and Biometrics provides products and services for identity and access management (IAM) and biometrics.

The Siemens DirX IAM suite helps customers grant and control the right access to the right people at the right time and to withdraw the authorization for this access when necessary – dynamically and across a multitude of IT systems and heterogeneous platforms.

Siemens has more than 15 years of experience in developing Identity and Access Management products and deploying them in customer projects around the world.

Customers in all sectors use the powerful products of the DirX family to automate their identity management processes and to meet the steadily growing demands related to governance and compliance.

Sales & Solution

Siemens
Enterprise Communications
GmbH & Co. KG

Hofmannstr. 51
81359 Munich, Germany
www.siemens.com/open

www.siemens.com

Products

Siemens AG
Siemens IT Solutions and Services
Identity Management and Biometrics

Otto-Hahn-Ring 6
81739 Munich, Germany
www.siemens.com/iam
identity.it-solutions@siemens.com

All hardware and software names used are brand names and/or trademarks of their respective holders.

© Siemens AG, 2008.
Right of modifications reserved.
07/08 | Printed in Germany