

[competence]

REFERENCE PROJECT

Security Automation And Integration
For a Large European Bank

_betasystems

[what]

IT auditors and the business organization staff of the bank agreed that for the 40,000 users of its client/server applications, IMS applications, other mainframe systems and its Windows network, the user administration systems currently in use were not providing the security required by the bank and were demanding too much administrator time. Additionally, the in-house developed application security system offered only limited administration capabilities not only making administration a tedious chore but also endangering the bank's security: monitoring of current user access rights was difficult leading to potential accumulation of access rights. Indeed, application security administration for the IMS mainframe systems and the Windows-based client/server applications was being performed manually or by using self-written scripts.

Automating and Integrating Network and Application Security

The bank chose SAM as a standard software solution enabling it to integrate network and application security, administer both in a uniform way, and to automate administrative tasks. SAM offers broad functional support for Windows and RACF administration and provides all the necessary customization means for efficient management of application security. As it was decided from the start that, later down the road, user administration would be role-based, SAM's uniquely strong role-based administration capabilities led it to become the clear choice for the bank. Its ability to combine rules and roles promised great potential for a high degree of automation.

SAM aConnect delivers standardized application security administration

When Beta Systems introduced SAM aConnect as a standard connector for application security administration, the bank soon decided to replace the initially customized application security support for their mainframe and client/server applications with the new product. With several of the product's features based on experiences made with the bank, it was an optimal fit with the bank's requirements of enhanced usability and standard software support.

SAM aConnect provides a generic administrative layer for application security. Natural language rules can be defined to determine which user can access which service or transaction ("access profile" rule set) to use which objects ("object profile" rule set). SAM's role concept and all of its provisioning features can be leveraged with SAM aConnect for easier administration and auditability of a company's application security.

With assets of over 380 billion Euros, the bank is one of the leading private business banks in Europe. It has app. 32,000 employees and almost seven million private persons and companies as customers.

[who]



SAM provides unparalleled automation

In a first phase, SAM was implemented and connected with the RACF systems together with other mainframe systems such as VM, TPX and TSO for which access rights had been maintained using an in-house tool. A connector for the support of the application security systems was developed (this was before SAM aConnect came onto the market) and the different user ID conventions were harmonized.

As a result, users and access rights could be uniformly, efficiently administered and the user ID consolidation served as the basis for further activities.

Windows integration, role-based administration and automation

The second phase had three important objectives: integrating the Windows network, creating a role concept and implementing sophisticated automation features.

Firstly, the Windows network of the bank was integrated within the SAM solution making SAM the governing authority for the systems with the largest numbers of users and the highest strategic importance for the bank.

At the same time, a role concept was created based on business processes, organizational parameters and the existing access rights. Besides a basic role for each job function ("cost center" and "location" became the key attributes for roles), several additional role categories were defined, like special purpose roles, roles for project groups, and roles for employees in their probationary period. The implementation of the role concept took less than a year. After having found the key role attributes, the existing access rights of groups of users with the same attributes were closely examined. Based on a frequency of occurrence approach, the potential access rights tied to a role were determined and verified. A positive side-effect was the ability to 'clean-up' existing access rights.

[how]

The role concept was used to implement sophisticated automation functions relying on SAM's provisioning engine. Changes in the HR system, occurring when employees join the bank, change their job or location, or leave the bank, are communicated to SAM, which performs the appropriate changes in user accounts and role connections. In addition, changes in the cost center structure and in the business processes are automatically transferred to SAM and produce changes of the role structure. The bank was able to automate almost 90% of routine administrative tasks.

Delegated Administration

The bank implemented an administration concept consisting of 3 types of administrators, all using personalized user interfaces, which could be easily configured with SAM: Several hundreds of IT-coordinators in local branches are today performing resets of forgotten passwords and user revokes/resumes. Branch administrators are maintaining user-role connections that are not automatically administered. Last but not least, central administrators are responsible for the maintenance of the role model and for remaining technical administration tasks.

SAP integration and support for organizational restructuring

After a period of productive use of the SAM solution, the bank decided to leverage the achieved administrative efficiency for its SAP systems as well. SAP systems were therefore connected with SAM so that the bank's SAP help desk could work with SAM's cross-platform help desk console.

[gain]

SAM saves millions of Euros each year

Today, SAM Jupiter is used to manage 40,000 users in several Windows networks, RACF systems, SAP systems, 2 mainframe and 3 client/server application systems, Unix systems, a directory and several smaller systems. About 1,000 roles are implemented, with inheritance for up to 3 levels. Each person has between 2 and 7 role connections, which are administered fully automatically except for a small few. SAM Jupiter's Provisioning Engine carries out several thousands of routine access rights changes per week. The bank's 90% automation rate for these tasks results in considerable cost savings for security administration and user management.

[experience]