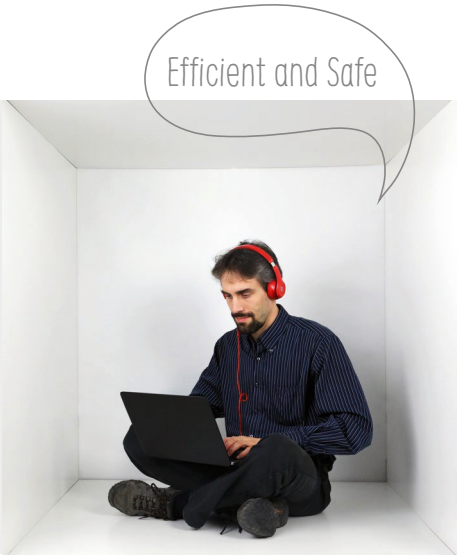
Identity Management (IDM) Deployment Case Study

One Password – One Role



Project goal: Effective management of user access rights - by connecting to the client's HR system, changes (adding, removing or changing an account) in applications will be made automatically with the entry or exit of an employee or a change in the employee's data (change of surname, promotion, etc.). The main focus will be on the speed, accuracy and traceability of the changes made. Among other things, this implies a significant reduction in the current number of user roles, which will make it possible to manage user permissions in enterprise applications.

CASE STUDY

IDM Technology

- **Microsoft Active Directory** (Windows domain) – manages workstation security.
- **Oracle Identity Manager** – central administration of identities and roles, integrated with the HR system, manages accounts and authorizations in VZP ČR corporate applications.
- **Oracle Enterprise Single Sign On** – component that ensures automatic filling in of names and passwords for technologically diverse business applications.
- **Oracle Virtual Directory** – component that provides the LDAP interface.
- **External and Consolidated Application Role Store** – a tailor-made database solution with LDAP interface for enterprise applications.

SERVICES PROVIDED

Other Goals of the Project

- **User Comfort (SSO)** – the client's employee will only need to know a single password for their normal work. All other application passwords will no longer be known and will be automatically managed and filled in by the IDM platform when logging into the enterprise application.
- **Uniformly Defined Level of Security** – the customer will be able to define a password policy across the spectrum of enterprise applications according to current security needs; thanks to the SSO, these changes will not be reflected in the work routine of employees.

Benefits

- Limiting the risk of „lending" a foreign identity
- Maximized user comfort thanks to Single Sign-On, ie the user is automatically logged in to applications
- Preventing of the existence „uncontrolled" application accounts
- Effective authorization management thanks to created company-wide roles (only tens of roles for 5,000 employees)
- Unified identity and authorization management processes across all territorial offices of the company
- The correctness and timeliness of the data is ensured through the rapid promotion of changes to all IT systems from an authoritative source – the personnel system
- Reduction of many application role stores - into one common consolidated repository that provides a standardized LDAP interface

Advantages

- Automatic login to all accessible applications based on a single authentication

GEM System | Štětkova 1638/18, 140 00 Praha 4 – Nusle, Czech Republic | sales@gemsystem.cz | www.gemsystem.cz

Integrated Systems

- Microsoft Active Directory
- Microsoft Exchange 2010
- Microsoft SharePoint
- Customized applications (Oracle Forms, Oracle DB)
- SAP R/3
- LMS (MS SQL)
- Cisco VPN
- Vema HR systém

VŠEOBECNÁ ZDRAVOTNÍ POJIŠŤOVNA ČESKÉ REPUBLIKY

(Public Health Insurance)

VZP ČR was founded in 1992 and has long-term been one of the main pillars of the Czech health care system. With more than 6.2 million clients, it is the largest health insurance company in the Czech Republic.

Characteristics of VZP ČR in Figures

- 5 000 employees,,
- 1 200 organizational units,
- dozens of enterprise systems (AD, Exchange, Oracle Forms, Oracle DB, SAP R / 3, MS SQL),
- an extensive network of branches,
- the most extensive network of contracted health facilities.

Hewlett Packard Enterprise

Main Integrator of the Project

A leading technology provider of printing solutions, personal computing, software, services and IT infrastructure.

ORACLE®

Worldwide supplier of integrated enterprise software and hardware systems.

- Extended client security standards
- Explicit assignment of user competences

Project Implementation

The implementation of the project, led by the main integrator Hewlett-Packard, consisted of both technological and process aspects. In the first case, it was the implementation and integration of individual IT systems, in the second case it was the redesign of the relevant corporate agendas. Due to the fact that the customer had been using Oracle products for a long time, the integrator of the Hewlett-Packard project decided to use IDM solutions of this brand. In addition, Oracle's wide offer in the IDM segment met all the prerequisites for the creation of such a solution that would cover the client's needs without fail.

Oracle Identity Manager is a key part of the solution. Once deployed in the customer's environment, it has become a kind of „central brain" that controls all user accounts and permissions in enterprise applications, including Oracle eSSO. It is connected to the customer's HR system, which has been assigned the role of authoritative element in the entire IDM solution. As a result, any changes to employee data are automatically reflected in the individual account data and user permissions. The HR system is now the only one with clear responsibility for the status of enterprise applications in terms of users and their permissions, which makes account management and administration much simpler and faster.

For this purpose, it was necessary to redefine the so-called corporate roles for the needs of the HR department. Now, HR managers can simply specify the different permissions for individual positions in the client's organisational structure directly. This has eliminated, among other things, the problem of multiple authorisations being cumulated, which previously occurred due to the succession of employees in several positions.

In particular, it is an effective identity and role management for more than five thousand employees based on automated propagation of changes from the HR system to other IT systems of the customer. This has rapidly reduced the volume of manual administration and covered the complete identity lifecycle (e.g. joining the company, changing positions, leaving the company, etc.).

From the user's point of view, the main advantage of the new IDM solution is clearly the automatic login to all available applications based on a single authentication when logging into Windows. The employee does not have to remember multiple passwords and can more easily switch between simultaneously running enterprise applications.

The IDM project also significantly increased the client's security standards. All application accounts are paired to specific employees, so activity performed under a given account has quickly and clearly identifiable responsibility. Linking IDM to the company's HR system also means that user responsibilities are clearly assigned and any changes to IT systems related to accounts and their permissions are traceable.