Evolveum

CASE STUDY | PUBLIC SERVICES OWNED BY THE STATE

Unified and Automated: How RMD Transformed Its IGA with MidPoint

The Road and Motorway Directorate of the Czech Republic (RMD) needed an identity management and governance system to enhance IT security, efficiency, and user self-service. To resolve these issues, RMD collaborated with IBA CZ to implement midPoint.

Overview

Challenge: RMD was looking for an IGA platform that would help them address the increasing requirements of IT security and eliminate manual processes to improve the efficiency of identity management and governance.

Process: IBA assisted RMD in implementing midPoint to optimize employee management, identity lifecycle, IT security, and compliance, while coordinating CAS and PAM deployment for single sign-on integration.

Outcome: The successful implementation of midPoint has led to automated identity management and governance, enhanced IT security, reduced costs, and ongoing improvement.

About The Road and Motorway Directorate of the Czech Republic

The Road and Motorway Directorate of the Czech Republic (RMD) is a state-funded organization that was established by the Ministry of Transport of the Czech Republic. The main scope of RMD's activities is to exercise the state's ownership rights to immovable property, which is made up of motorways and class I roads, to ensure their management, maintenance, repair, construction, and modernization.

The IT team administrates 6,000 enterprise identities and more than 94,000 roles.

The Objective

The need to implement an identity management system was driven by the Cyber Security Act and the ever-increasing requirements of IT security. RMD also wanted to improve the efficiency of internal administration and management of access permissions for application users, establish user life cycle management, and increase automation.

The Challenge

RMD was using a homegrown identity management system that lacked many features that would improve security, reliability, and speed.

The system lacked the possibility of having a consolidated user and permission overview as well as an option to generate reports. There was separate management of permissions in individual applications, and an extremely time-consuming recertification of permissions took place when an employee moved within the organizational structure.

The self-administration of users was not possible, and the IT department needed to repeatedly assign or modify individual user permissions manually based on requests. Users didn't have access to basic functionalities like password resets, resulting in a strained IT department with an increasing amount of repetitive demands.

Another challenge presented itself in the form of data inconsistencies caused by the fragmented management of personal data across multiple applications. Unification and validation of personal data (especially contacts) were complicated or impossible.

There were no tools or definitions of formal processes to support identity lifecycle management. It became clear that the system needed to be replaced by a centralized identity management and governance platform.

Key customer requirements were defined:

- To set up access management policies and their enforcement (RBAC matrix).
- To specify and implement organizational processes for identity lifecycle management.
- To have a full-featured graphical user interface available for user self-administration.
- To generate audit records and logs and evaluate them in SIEM.
- To enable real-time and retrospective reporting and monitoring of user permissions.
- To manage permissions on shared folders, especially permission handling after an employee has left the organization.

The Process

The project was considered highly complex, and IBA assisted RMD every step of the way. They started with a detailed analysis of their environment and identified possible risks and sensitive areas. This was followed by creating a catalogue of requirements for the final solution and writing a thorough solution specification that later became the basis for midPoint's implementation.

The following project objectives were set:

- The automation and optimization of employee management processes.
- The establishment of comprehensive identity lifecycle management.
- Inventory and management of organizational (business and application) roles.
- The order in the employee system and organizational structure.
- The introduction of auditing employees' and external contractors' IT activities.
- The improvement of the basic level of IT security in the organization.
- The establishment of a unified and clear inventory of internal and external identities.
- The central management of all user permissions in a single application.
- Increased efficiency of permissions management, automation, and minimum human error.
- Compliance with the requirements of cybersecurity laws.
- The establishment of a set of rules for the introduction and integration of new applications into the organization.

MidPoint was chosen because it could address all of RMD's challenges, and it also fits well in regards to the defined project objectives. MidPoint's flexibility in defining identity processes together with self-service capabilities were key aspects supporting this decision.

Along with this project, the CAS and PAM system deployment project was underway, requiring coordination and collaboration with RMD's implementation team

and their supplier. The joint effort was to make single sign-on operational. IBA CZ supported this activity by integrating midPoint using standardized connectors and connectors they developed specifically for the customer's end systems.

The Outcome

IBA CZ has successfully implemented midPoint at RMD, and it has been in production for a couple of years now.

RMD has implemented roles for each individual construction site for which they need to manage access. This allows for simple and immediate access to information about users and their permissions.

Now there is an automated and unified way to manage identities and access permissions to applications used in the organization. An approval workflow has been implemented across all departments in the organization to assign permissions. While significantly reducing the cost of managing permissions, RMD has also gained greater control over access, the ability to monitor and evaluate user IT activity, and the ability to generate a diverse range of reports, statistics, and regular audits in an automated way. This also allows reporting, permissions assignment, and the management of other user activities.

Thanks to midPoint's self-service features, the burden of excessive manual processing requests has been eliminated, and operational and administrative costs associated with managing permissions have been reduced.

With the introduction of standardized processes and automation, the identity lifecycle management for employees and contractors has been accelerated. IT security has increased dramatically, and the risk of security incidents has been reduced.

The cooperation between RMD and IBA CZ is still ongoing. They continue to develop and adapt the platform to the present requirements of the organization and expand it to include other end systems.

About IBA Group

IBA CZ and IBA Slovakia are technology companies specializing in providing comprehensive services in the field of software development ranging from consulting and custom development to services. They are both part of the multinational IBA Group.