Manuals+ — User Manuals Simplified.

beta systems

The IAM as a communication interface

Insurance Company
Merkur Versicherung AG relies on
Beta Systems Garancy Identity Manager as
central management tool for authorizations

merkur VERSICHERUNG

Project Overview

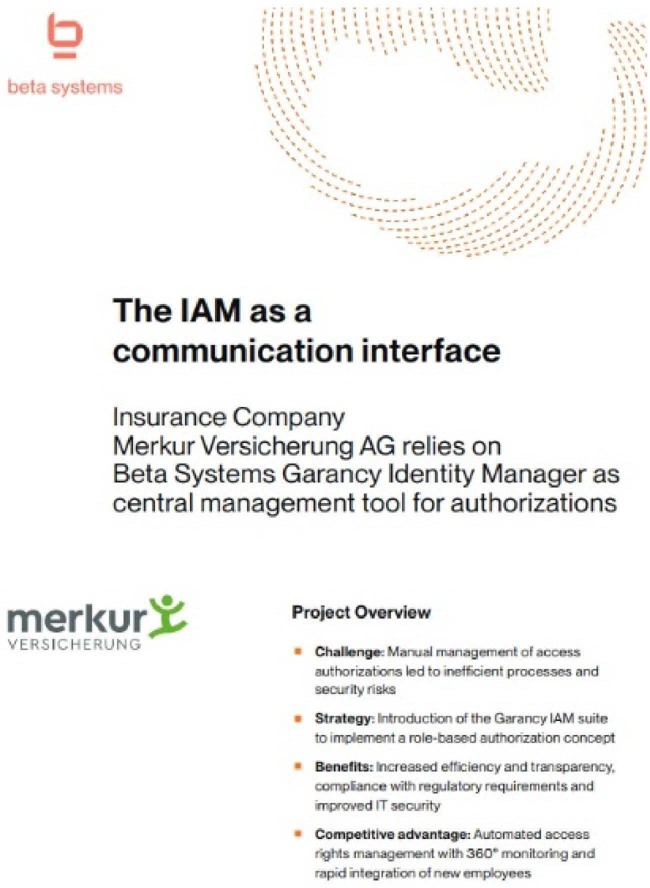
- **Challenge:** Manual management of access authorizations led to inefficient processes and security risks
- **Strategy:** Introduction of the Garancy IAM suite to implement a role-based authorization concept
- **Benefits:** Increased efficiency and transparency, compliance with regulatory requirements and improved IT security
- **Competitive advantage:** Automated access rights management with 360° monitoring and rapid integration of new employees

beta systems Garancy Identity Manager Instructions

Home » beta systems » beta systems Garancy Identity Manager Instructions

Contents

beta systems Garancy Identity Manager



beta systems

The IAM as a communication interface

Insurance Company
Merkur Versicherung AG relies on
Beta Systems Garancy Identity Manager as
central management tool for authorizations

merkur VERSICHERUNG

Project Overview

- **Challenge:** Manual management of access authorizations led to inefficient processes and security risks
- **Strategy:** Introduction of the Garancy IAM suite to implement a role-based authorization concept
- **Benefits:** Increased efficiency and transparency, compliance with regulatory requirements and improved IT security
- **Competitive advantage:** Automated access rights management with 360° monitoring and rapid integration of new employees

Specifications

- **Deployment Options**: On-premises or cloud-based (Garancy@Cloud).
- **Scalability**: Supports organizations of all sizes, adaptable to industry-specific needs (e.g., banking, logistics).
- **Integrations**: Compatible with HR systems, Active Directory, Azure AD, and other IT environments.
- **Compliance**: Tailored for regulatory standards such as GDPR, MaRisk, and BAIT Beta Systems.

The IAM as a communication interface
Insurance Company
Merkur Versicherung AG relies on Beta Systems Garancy Identity Manager as central management tool for authorizations

Project Overview

- Challenge: Manual management of access authorizations led to inefficient processes and security risks
- Strategy: Introduction of the Garancy IAM suite to implement a role-based authorization concept
- Benefits: Increased efficiency and transparency, compliance with regulatory requirements and improved IT security
- Competitive advantage: Automated access rights management with 360° monitoring and rapid integration of new employees

Insurance Company Merkur Versicherung AG relies on Beta Systems Garancy Identity Manager as central management tool for authorizations

In 2019, the insurance company made the When Merkur Versicherung was founded in Graz in 1798, the Holy Roman Empire under Emperor Franz II was in its final stages. This makes today's Merkur Versicherung AG, head

– quartered in Graz, undisputedly the oldest insurance company in Austria — but at the same time always at the cutting edge of technology and organization. With the IAM solution from Beta Systems, the insurance company now has complete control over who accesses which systems and when. This means that it meets all the requirements of the Financial Market Authority and streamlines internal workflows at the same time.

While other companies were still considering how best to distribute paper inboxes during the pandemic, Merkur already had an "eWork-place" — an electronic workplace that receives correspondence exclusively in digital form and forwards it to the right employee via an automated workflow. "Our IT landscape has grown by many such applications in recent years," says Ms. Kainz-Kaufmann from the Information Technology — IT Management department. The following applies to all of them: it must be determined who has which access to a system and for how long. Previously, these authorizations were granted via a ticket system (Jira). There, the specialist department had to create their requirements for who was allowed to use which software and to what extent as a ticket, and the administrators of the individual target systems then implemented these for the individual users in the systems.

In the past, authorizations were not based on roles, but on people. This meant that an individual ticket was created for each authorization request and there was no common overview of who had which authorizations and when. "For external audits, we always had to search for this information from the individual systems or from the ticket management system," says Eva Kainz-Kaufmann. Not least for security reasons it is essential to know at all times who has which rights and where, and that these can be granted and revoked just as quickly as they can be withdrawn.

Maximum flexibility when connecting self-developed applications
In 2019, the insurance company made the decision to introduce a central administration tool for authorizations. A market evaluation was carried out together with an external consulting firm. Out of an initial ten manufacturers, three were shortlisted, with Beta Systems ultimately winning the business with its Garancy IAM suite. In addition to the Merkur Information System, Lotus Notes, eWorkplace and Microsoft Active Directory (including other connected systems) had to be linked to the IAM software.
„ Beta Systems' Garancy IAM suite was the only product that integrated seamlessly with our proprietary core insurance software.

Nikola Birkic
IAM-Administrator

Implementation of the role concept as a first step
Parallel to the introduction of the Garancy IAM suite, Merkur Versicherung AG began to develop a new role concept. Existing systems and IT authorization structures were re-viewed and cleaned up from the ground up. Which accesses for certain folders, files or systems only exist because someone created them at some point? Which authorizations must be deactivated and which must remain in place? The role concept created the basis for making such decisions.

With the introduction of the Garancy IAM suite, new authorizations are now only assigned based on roles. The insurance company creates the roles in the Infoniqa HR system. Which employee started when, in which department does they work and what position does they hold there? Based on this information, each employee is assigned two basic roles, the organizational role and the business role (corresponds to the job profile). The organizational role basically defines the department in which someone works, while the business role describes the exact activity. This classification was carried out by IT in consultation with the system owners and the divisional managers of the respective department.

The role assignment in HR already existed in a rudimentary form. But the users had to be created manually in the ticket system and in the individual applications, nothing happened automatically. Now Infoniqa automatically transfers the role profiles to the IAM system, which assigns them the appropriate authorizations — a clear hierarchy.
Says Nikola Birkic, "We defined this in many discussions with the respective manager and have been reviewing it regularly ever since. Our managers must regularly check whether there have been any changes to the roles or tasks via the Garancy recertification process."

Supervisors manage authorizations for their teams independently

In addition to the two standard roles, there is also a functional role. Managers can use them to assign or withdraw finely granulated access to individual systems to people with the same organizational and business role, for example for individual projects or in the event of sick leave. In total, over 1,000 roles have been set up at Merkur Versicherung. Since the beginning of 2022, one department after another has been brought on board, where team managers can independently manage authorizations for their team members via the Garancy portal, independently of IT. For Sandra Weiß in the Customer Services department, for example,"the tool is a blessing", as Nikola Birkic reports. The larger the department, the more often you have to set up vacation replacements, which Sandra Weiß can now do herself on an ad hoc basis using the function roles in the portal. Previously, she had to submit a Jira ticket for this.

This means that the IT department has less work and can handle audits with ease. At the same time, it is guaranteed that if someone leaves or moves within the company, they cannot automatically unjustifiably take their authorization from one department to the next. Merkur Versicherung AG thus fulfills all important IT security standards.For example in some projects, only the project owner should have access to the folder after one year. Setting this automatically is the task of the IAM system.

In Garancy, start and expiration dates can be entered for which a role is to be assigned; manually initiating such changes in the ticket system is a thing of the past. The use of the Garancy Access Intelligence Manager enables 360° dynamic monitoring and a historical view of data on access rights and associated risks. The insurance company's IT department can display reports on the review of authorization structures in the company and the identification of potential access risks and perform multidimensional analyses — a unique selling point of the Beta Systems solution.

Garancy brings operational organization and HR on board

At the beginning of the role lifecycle, when onboarding a new employee, it used to take several days to create all the accounts and peripherals for them. The line manager first had to create a ticket, which was then implemented by the individual IT administrators. Now, as soon as the HR department has entered the new employee's data in the HR system, IT receives it directly via the IAM. In this way, Garancy brings the operational organization and HR on board — whatever is created or changed there has a direct and immediate effect on the IAM system. It thus becomes the communication interface between the organization, HR and system administration.

Merkur Versicherung's entire IT landscape runs in an external data center. The Beta Systems specialists also implemented the IAM solution there, set it up and carried out the training — all completely remotely. Of course, there were small hurdles, including the connection of target systems if they do not allow access to the Beta Systems interface. In 2022, the Merkur Group took over Nürnberger Versicherung AG's Austrian business, and the approximately 120 employees joined the Group in the same year. That meant some additional preparatory work

was needed. New roles had to be created for these employees. As soon as the new additions were managed in the HR system, the IAM solution takes over the management and assigned the roles their respective authorizations. This meant that the new colleagues were immediately integrated — faster than would ever have been possible in the past using a ticket system.
„ Beta Systems always found a creative solution, and in an impressively short time.
All in all, a very pleasant culture of discussion.

Martin Majhen

IT Manager

The company
Merkur Versicherung AG, headquartered in Graz, is the oldest insurance company in Austria and insures people’s lives, health and assets. Its core competence lies in the area of health care. In addition to the Merkur Campus in Graz and three sales offices, there are also several branch offices in each province. Around 1,000 employees work for Merkur Versicherung in Austria. It is also represented by its subsidiaries in Slovenia, Croatia, Serbia and South Tyrol.

Facts & Figures

- Year founded: 1798
- Employees: approx. 1,000
- Head office: Graz
- Chairman of the Executive Board: Ingo Hofmann

Industry
Insurance

The challenge
Merkur Versicherung AG used to regulate authorizations for access to IT applications via a ticket system; the administrators of the individual target systems then implemented these manually for the individual users in the systems.

Products employed
GARANCY Identity Manager, GARANCY User Center, GARANCY Recertification Center, GARANCY Access Intelligence Manager

Benefits of the Beta Systems solution
With the introduction of the Garancy IAM suite, new authorizations are now only assigned on a role basis. Supervisors can manage the access rights for their team members independently via the Garancy portal. This means a high degree of flexibility for the specialist departments while at the same time reducing the workload for IT.

Competitive advantage
Thanks to the use of the Garancy IAM suite, Merkur Versicherung AG can now look forward to audits with peace of mind. Without the solution, these would previously have always meant lengthy investigations. Now there is more time for customer-oriented activities. Acquisitions such as Nürnberger Versicherung are organized much faster.

Key figures

- Connected systems: ten in the first step, planned all
- Roles set up: approx. 1,000
- Managed user accounts: approx. 6,322
- Duration of implementation: 24 months incl. preparation

FAQs

- **Q1. What industries benefit most from the Garancy Identity Manager?**
  The platform is particularly effective for industries requiring stringent data governance, such as finance, insurance, healthcare, and logistics Beta Systems .
- **Q2. Can the system be deployed in hybrid environments?**
  Yes, Garancy Identity Manager supports on-premises, cloud-based, and hybrid deployments, offering flexibility based on organizational needs Beta Systems .
- **Q3. How does Garancy ensure compliance?**
  It automates access rights recertification, role-based assignments, and audit reporting to help businesses comply with regulatory standards like GDPR and BAIT Beta Systems .

Beta Systems Software AG Alt-Moabit 90d, 10559 Berlin

- Tel. +49 (0) 30 726 118-0
- **www.betasystems.com**, **info@betasystems.com**

Documents / Resources

 beta systems **The IAM as a communication interface** Insurance Company Merkur Versicherung AG relies on Beta Systems Garancy Identity Manager as central management tool for authorizations merkur VERSICHERUNG **Project Overview** **Challenge:** Manual management of access authorizations led to inefficient processes and security risks **Strategy:** Introduction of the Garancy IAM suite to implement a role-based authorization concept **Benefits:** Increased efficiency and transparency, compliance with regulatory requirements and improved IT security **Competitive advantage:** Automated access rights management with 360° monitoring and rapid integration of new employees beta systems Beta Systems Software AG Alt-Moabit 90d, 10559 Berlin Tel. +49 (0) 30 726 118-0 www.betasystems.com, info@betasystems.com	beta systems Garancy Identity Manager [pdf] Instructions Garancy Identity Manager, Identity Manager, Manager

References

- User Manual

Manuals+, Privacy Policy