

Insurance MFA case study – on-premise and multiple integrations

Leading insurance group Uniqa uses SecurEnvoy MFA for secure sign-on to all applications by remote workers and partners.



About the Company

UNIQA Czech Republic is part of one of the leading insurance groups, UNIQA, located in Austria, Central and Eastern Europe and was set up in 1993 in the Czech Republic. UNIQA Czech Republic offers personal, property, commercial and industrial insurance and has a nationwide sales network comprising of its own sales representatives, customer offices, brokers, agents and vehicle dealers.

Challenge - security of user identities

Looking to standardise and increase the security of user identities, the insurance company decided to use additional security tools, including multi-factor authentication.

UNIQA started to consider using multi-factor authentication as part of a security compliance and standards initiative led by the head office based in Austria. The aim of the project was to ensure secure sign-on to their systems by remote workers, not only employees but also distributors and other partners. To meet their requirements UNIQA was looking for a solution that would provide a single platform for integration with all their different systems.

The main requirement was independence from external systems, but with the ability to be able to integrate external systems in the future. Ease of use, different types of authentication (push notification, use of smart phones etc.), high availability and integration with directory structures such as Microsoft Active Directory and especially OpenLDAP were all key for UNIQA.

Insurance MFA solution - evaluated and selected

During the selection process, UNIQA looked at different multi-factor authentication solutions and after detailed analysis they chose the MFA solution from SecurEnvoy which met their strenuous requirements.

It was very important from a security perspective for UNIQA to have an on-premise only solution, and they found that some solutions were not entirely on-premise and that many vendor solutions save data to the cloud. SecurEnvoy meets this requirement.

In addition, SecurEnvoy MFA was selected by UNIQA for its user-friendly environment with push notifications, Android app integration and its wide range of authentication methods, including SMS, hardware tokens and use of modern technology, such as smart watches, which although not required immediately, could be used in the future.

UNIQA very much appreciated SecurEnvoy's flexibility and support in meeting their specific integration requirements.

The deployed solution also needed to meet their vision of "protected access for all customer partners", requiring protection for several thousand identities.

MFA Implementation - across a partner network

UNIQA chose Czech partner M-COM s.r.o. to implement the project. M-COM is a key business partner of Comguard (SecurEnvoy's distributor for the Czech Republic and Slovakia). M-COM were tasked with handling some specific requirements for integration, including HCL Domino, HCL Verse and Zimbra, which are not typically integrated into SecurEnvoy MFA.

Another challenge was the wide range of different users and systems. Two-factor authentication not only needed to be connected to the customer's internal system and used by employees and partners, but also by the suppliers that the insurance company works with.

The project implementation confirmed that the solution can be deployed relatively quickly and easily and can be connected to a wide range of supported technologies. Knowledge of third-party technologies was also important for integration.

Result - user-friendly MFA solution that delivered

Following successful implementation, UNIQA updated its users about the importance of multi-factor authentication, and they saw a real advantage in having a user-friendly solution like SecurEnvoy MFA that is easy to use and not a frustrating barrier for adoption.

Even though there is a wide supply of market choice, due to the requirements that were placed on the solution, the final choice of supplier was relatively clear. The SecurEnvoy solution proved to be a very good choice with regards to price, technology and performance.

The customer appreciated the high quality and level of support from the vendor and partners.

Solution Highlights

- **Single platform supporting a large number of different systems and integrations (including: OpenLDAP, Microsoft Active Directory, Forcepoint VPN, Microsoft Office 365 and HCL Domino)**
- **Wide range of authentication options, including push notification and Android App**
- **Fulfils requirement for an on-premise only solution that does not save data in the cloud**
- **Improved security with MFA solution supporting remote workers (employees, distributors and partners)**

[Download Success Story >](#)



The SecurEnvoy solution proved to be a very good choice with regards to price, technology and performance.