AIRLOCK

Migros
Centralised SAP portal for suppliers

Migros is an inherent element of daily life for many people in Switzerland: Some 1.4 million customers shop every day in the supermarkets and stores run by the long-standing company founded in 1925. Migros is at the same time also the largest employer in the alpine country with some 84,000 employees. In 2008 the group posted profits of 701 million Swiss francs and their market share totalled more than 20 percent for the first time.

However, following the entry of international commercial chains into the Swiss market, Migros is now confronted with increasing competition. The up step in dynamics and the ensuing price war forced the group to adopt a uniform merchandise management system and to standardise its IT systems using SAP for Retail several years ago. In order to make the processes for bid proposal management more efficient, both the national and the international suppliers were to be given the opportunity of submitting their offers directly into the SAP system and of taking part in auctions as from 2008.

Centralised SAP portal with preceding authentication

"The specifications were clear: Simple access for our suppliers to SAP's Supplier Replenishment system," says Peter Rieder, manager of IT infrastructure services at Migros IT Services. "The following challenges resulted from an IT perspective: Secured authentication for users and allocation of access authorisation, protection of the internal SAP server against unauthorised access attempts and user-friendliness by integrating the diverse backend systems into one centralised portal."

It was not a viable option to make the SAP server directly available to suppliers via the internet, particularly because Migros would then have had to ensure that the suppliers opened the corresponding communications ports – and in view of the high number of companies spread across the globe this would have been both a tremendous expense and a security risk, because then each server would have a public IP address. Furthermore, the backend systems should be accessible under one single succinct URL in order to simplify the operations.

Although Migros has its own Certificate Authority and Public Key Infrastructure (PKI), one did not wish to dictate the use of specific client certificates to the companies or to support further authentication methods additionally. "Client certificates - as they are used by Migros internally - guarantee a high level of security," comments Peter Rieder. "If a company has suppliers across the globe, then it needs a safe and yet straightforward solution. Certificates are without doubt secure, but by no means simple. We wanted to avoid having to explain the installation on a Chinese PC to a Chinese supplier, so we opted for alternative authentication methods with graduated authorisations in our basis specifications."

Single sign-on for suppliers with Airlock

Since the Migros IT team keeps up to date with new technologies, they came across the web application firewall Airlock during the course of their evaluation phase, explains Peter Rieder: "Migros uses alternative products in other areas so we were already aware of their limitations and

Company Facts

Sector	Trade
Founding year	1925
Earnings 2008	**CHF** 25,75 billion
No. of employees 2008	84 096
Members (of the cooperative)	2 055 044

knew that they could not give us the flexibility we were looking for. Our attention had also been drawn to Airlock some time ago as part of our ongoing market observations – and now the SAP portal project got underway."

When we made competitive comparisons, we were also convinced by Airlock's flexible support for different authentication methods for single sign-on on the SAP portal. Under the preceding authentication, users login to Airlock today with a client certificate, and login/password – in the near future they will also be able to login with one time passwords (OTP). Authorisations are assigned accordingly: All internal and external users are compiled in a meta-directory. There is one group per application, whereby suppliers can be in one or several of these groups depending on their authorisation levels. Airlock checks the certificate and the user's group affiliation via the LDAP server and meta directory before releasing the application. If an OTP is being used, then Airlock checks the login/password in the meta directory first as well as the challenge on the token server. Airlock currently supports three authentication methods. These will probably be complemented by an anonymous access with significantly reduced authorisation.

Different certificates and Login-Mapping

Certificates from suppliers, which do not have to originate from Migros, are installed on the meta directory, so that Migros can check their validity at any time. If a supplier is no longer valid, then the certificate is deleted from the meta directory. "This procedure demands a lot of flexibility from Airlock because our tree in the meta directory does not correspond exactly to the respective specifications on the certificate, but the solution has proven itself in operation and works perfectly." Another obstacle that has been successfully negotiated: Migros stipulates that the mail address is used to login, but SAP supports neither the @-sign nor more than eight letters for logins. Airlock thus maps the logins in the meta directory to SAP user names.

Following the successful authentication, suppliers access the central SAP portal behind which the individual servers are installed. Users are only given access to those functions for which they are authorised.

All URLs lead to Airlock

Viewed from the outside, all links always lead to Airlock so direct access to the SAP server is prevented. This is possible because Airlock rewrites all internal URLs – this works although SAP uses absolute URLs and is therefore not capable of reverse-proxy in itself.

The largest challenge for the implementation is, according to Peter Rieder, the searching and rewriting of the URLs as well as the filter adaptations: "This is, of course, a complex issue that we have managed to resolve together with the Airlock support team."

Despite the smooth implementation one question remained unanswered: What happens if SAP releases a major update? "I can speak from experience here, because we recently implemented just such an SAP update at Migros. The result: Only two rules had to be adapted on Airlock, otherwise everything continued to run smoothly,"says Peter Rieder.

Airlock at Migros: More than SAP

A centralised SAP portal and preceding supplier authentication are important areas of use for Airlock at Migros, but by far not the only ones: For example, invoices for Migros industrial companies are scanned in and saved in electronic form on the server. Different people are then assigned the necessary controlling and approval visas using a workflow. In order to ensure that it is the right user, Airlock is used to check the certificates here.

There are also plans to expand the portal with additional SAP applications from the marketing area and other processes. In the long-term users should be able to access a whole "world" of functions using single sign-on: "In specific terms, the first issue is the integration between SAP and Microsoft Sharepoint on one presiding portal. So during the evaluation phase, we made sure that Kerberos can be supported too – and Ergon was the only manufacturer that could guarantee this for us," says Peter Rieder.

The Airlock Team has already proven that this can be achieved with a proof-of-concept that was, according to Migros, implemented in just one day. Airlock uses the certificate to identify the user and his authorisations and then releases a Kerberos ticket from the domain controller. The user needs this ticket to access Microsoft Sharepoint and at the same time it can also be used in this specific instance to register on the SAP portal, too. The session access is run via cookies. Peter Rieder comments: "We have managed to merge two application worlds using single sign-on and certificates. Airlock convinced us in a very short period of time."

Best teamwork

During the course of complex projects challenges inevitably arise which cannot be resolved according to the book – and this is when the hour strikes for support. Working with a Swiss manufacturer is, according to Peter Rieder, advantageous in several different ways: "Looking back, I have to say: Having a manufacturer close by is worth its weight in gold. It is not just the geographical proximity that is positive, but also the same cultural background, such as, for example, quality expectations. My experience has also shown that the commitment for implementing the customer's wishes is also higher, Airlock is the best proof of this."