actidoo

Introduction of an Identity & Access Management System (IAM) for external users

Case Study

ActiDoo GmbH (ActiDoo) introduced Keycloak as an Identity & Access Management System for customers and other external users (C-IAM) at Schüco International KG (Schüco).

This centralized user administration has made it possible to establish a uniformly high level of security, significantly increase the speed of provisioning and deprovisioning processes and considerably reduce the administrative effort involved in assigning authorizations.

In a self-service portal, users can change their access data and customer administrators can manage the authorizations of their employees themselves. This helps to reduce the workload of service employees. Uniform branding of the login screen used in the connected services and the self-service portal increases the recognizability of Schüco and user confidence in the services offered. Thanks to modern single sign-on (SSO) procedures, users only have to log in once and are then already logged in to all other services.

Customer

SCHÜCO

- Schüco International KG
- System provider for windows, doors, facades
- over 6,000 employes

Technologies used

- Keycloak, incl. customizing & branding
- PostgreSQL
- Docker
- Active Directory

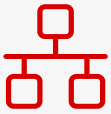
Project

- Conception, planning, implementation
- Migration and consolidation of existing user master data

The task

Schüco offers several digital services for various target groups (fabricators, architects, suppliers, etc.). These services are provided by different specialist departments using different technologies

Before the start of the project the login was implemented by each service itself. The user master data for the services was obtained from various sources, but in most cases originated from an SAP Hybris e-commerce system that acted as a customer portal. To supply the various applications with this user master data, there were various interfaces in the Hybris system, some of which were developed in-house. Password verification was partly carried out by such an interface, but partly by the applications themselves. Since all user interfaces and user data processes mapped in Hybris were individual developments that did not conform to any standard, the connection of each new system was complex and time-consuming. User deprovisioning was also insufficiently automated overall and therefore too time-consuming. Schüco had therefore been considering mapping the user data processes of external users centrally in a suitable system for some time.



> 20
Connected services

> 200.000
Managed identities

Against the backdrop of an upcoming cloud migration of the Hybris system to the modern SAP Commerce Cloud platform and the associated complete reimplementation of the customer portal, it happened to be the perfect time to introduce a new system that could take over the identity provider function and offer additional IAM functions. On one hand, the introduction of the new system was intended to increase convenience for users, e.g. through single sign-on and a standardized login for all services. On the other hand, a standards- based, very high level of security was to be ensured for all applications and a single point of truth was to be created in which user master data and authorizations could be maintained centrally. Authentication and authorization were to be handled via standard interfaces. A particular challenge was the high time pressure due to the fixed deadline for the end of the license of the existing Hybris system and the high coordination effort between the many application managers involved.

As Schüco attaches great importance to the recognizability of its brand and a uniform appearance, the system was to have extensive branding options.

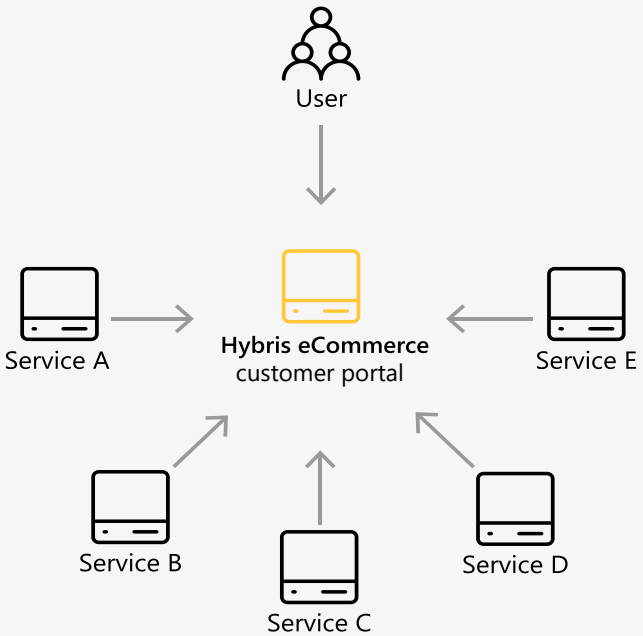
The solution

Detailed analysis

Schüco commissioned ActiDoo to design, plan and implement the introduction of an identity and access management system for all external identities, including the migration of existing data. To begin with, a detailed analysis of the existing user data flows and the authentication and authorization landscape at Schüco was carried out. The onboarding processes were also considered. The result was a complete and widely ramified network of dependencies among the systems with a high proportion of individual development with regard to login and interfaces. However, the majority of user data was stored in Hybris, which was clearly the center of the network. As it turned out, an additional requirement was that some of the processes also had to be carried out by internal users, who are treated exactly like external users, but should be marked as internal users for the applications.

The decision was made to set up a Keycloak cluster, which is particularly characterized by its flexibility as well as its branding and customizing options. The system is operated in a Docker container and is ready for a cloud move of the Schüco infrastructure planned for the future. DevOps processes ensure that new versions of the customizing can be rolled out in the shortest possible time at the push of a button without downtime.

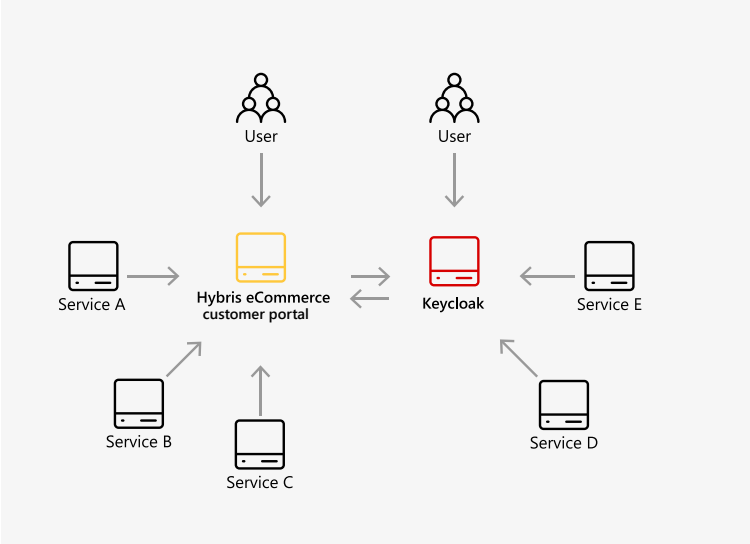
Network before conversion



Multi-step process instead of BigBang

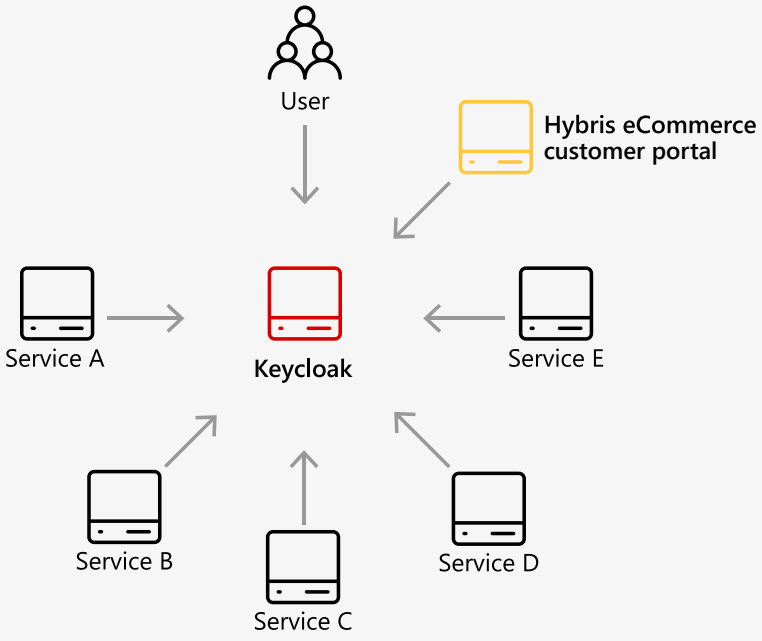
As it quickly became clear that not all applications could be converted at the same time, thus ruling out a big bang scenario, ActiDoo designed a multi-step process for the introduction of the Keycloak system with a transition phase in which parallel operation between Keycloak and Hybris as the user master data system was planned.

For the external users, ActiDoo developed a bidirectional synchronization of the user data including the password hashes with the Hybris system as well as an extension for Hybris that enabled Hybris to support the more modern hashing methods used in Keycloak and established parallel operation of Keycloak and Hybris. A user that was created or changed in Keycloak therefore also functioned in systems that were already connected to Keycloak and vice versa.



In this way, the applications could be connected to Keycloak step by step. They were also independent of the conversion of the registration process to the Keycloak system.

Final network



Active Directory

To connect the internal users the Active Directory has been linked. An extension developed by ActiDoo was used, which significantly improves the performance of LDAP user queries compared to the standard.
The Active Directory authorization groups have been retained for internal users and can be evaluated for authorization. For example, certain Active Directory groups automatically allow access to certain applications.

Branding und Self-Service-Portal

ActiDoo branded also the login screen and the self-service portal where users can view their logins and change user data themselves. There, ActiDoo implemented a B2B user administration that allows administrative users of a customer to invite new users from their company, remove users from the company or manage certain authorizations of their company's users themselves.

Overview of the procedure

1.Analysis
- Recording the ACTUAL situation
- Stakeholder analysis
- Risk analysis

2. Goal
- Conception of the TARGET situation

3. Plan
- Planning the structure of the migration
- Conception of the transformation process
- Creation of a roadmap
- Planning the CutOut scenario

4. Setup
- Setup and configuration
- Implementation of parallel operation

5. Migration
- Intensive care
- Support with the connection of services

6. CutOvertion
- Shutdown of the old system
- Production operation with maintenance

The result

ActiDoo successfully implemented the C-IAM system within the planned time and budget and also actively supported the developers of the applications to be connected to Keycloak.

Schüco customers, suppliers and partners now use the same login for all connected services and a standardized self-service portal to manage their user data. After the first login, they automatically have access to all other services available to them without having to log in again.
Since only the Keycloak system has direct access to user login data and all external users are managed uniformly via Keycloak, a uniformly high, centrally managed security level could be achieved.

The security level can be implemented. Adjustments to the security rules have a direct effect on all connected systems. New users are immediately available in all connected services, depending on their authorizations, and can be deactivated centrally just as quickly.

As the central master data administration for user data, a single point of truth has been created in this way. Standard interfaces such as OpenID Connect and SAML guarantee that new systems can also be connected quickly. Technologically, the Keycloak Cluster is well prepared for use in the cloud thanks to its operation in the Docker Controller.

Customer feedback

I am convinced that the success of the project is largely due to the expertise of the Keycloak experts at ActiDoo. They quickly found an excellent solution for every application and demonstrated impressive know-how on the subject of modern authentication procedures. The holistic view of the ActiDoo experts and the collegial cooperation were the key to success. A subsequent penetration test by a third-party company confirmed the high level of security.

Benjamin Heiland
Product Manager IT Sales Cloud Solutions
Schüco International KG
SCHÜCO

actidoo

About ActiDoo

Based in Paderborn in the heart of East Westphalia, ActiDoo GmbH supports its customers worldwide in the implementation of their digitalization plans. As an agency for digitalization, it is primarily active in the areas of enterprise application development and identity & access management. The company's experienced developers and consultants rely on a mix of the latest technologies and proven development concepts. In this way, they implement the individual wishes of their customers promptly, efficiently and to the highest quality.

Do you have any questions or suggestions?

Please feel free to contact us

To the contact formular

info@actidoo.com

05251 5449490