univention
be open.

# Identity & Access Management as a Key Component of Modular Software Products

# Identity & Access Management as a Key Component of Modular Software Products

Modular software products offer the flexibility and future-proofing that modern IT architectures require. However, ensuring their smooth integration into existing systems demands a well-thought-out strategy. It's important to avoid the potential pitfall of increased complexity that modularization can bring.

---

## Contents

# 1. Starting Point: Modular Software and Legacy IT

In modern application development, a modular software architecture — where functions or functional areas of an application are divided into separate software modules — is the standard approach. These modules are independent units, each performing specific tasks or functions within the application.

## Reasons for Modularization

- **Encapsulation:** Modules operate independently, enhancing security by ensuring that an error in one module does not directly impact others.
- **Scalability:** By separating functions into modules, the application can scale more effectively, targeting redundancy and resource allocation where needed. This leads to more efficient use of data center resources and confines scaling issues to individual modules.
- **Innovation:** New features can be added through additional modules, and existing modules can be updated or replaced without altering the entire application.

## Integration into Existing IT Landscapes

When a modular application is deployed to a user organization, they typically expect only a few clear interfaces for integration with their existing IT infrastructure. Integration should be a one-time process, not something that needs to be repeated for each module of the application. This means the application as a whole should integrate seamlessly into the existing IT environment, without requiring adjustments for every module update or addition.

# 2. Key Aspect of Integration: Identity Management

In applications, identities are pivotal. They represent end users who interact with the application or exchange data, often through other software systems used within an organization. Most application interfaces require that access is conducted through a verified, or authenticated, identity, such as when a user accesses a protected document. This authentication is critical for ensuring secure access.

It can be assumed that most IT environments already have Identity & Access Management (IAM) systems in place to manage identities and their permissions within the organization. These systems also define organizational structures such as workgroups, teams, and hierarchies. A new application should make use of this existing information to map predefined permissions and relationships between identities within the application, sparing end users from having to recreate structures like workgroups. Therefore, any application must be able to connect to the primary IAM system to ensure quick, secure, and user-friendly integration into the existing IT landscape.

# 3. Challenge: Ensuring Modularization Doesn't Lead to Complexity

In modular software applications, most modules require information from existing IAM systems. These modules can interact individually with the established systems through open interfaces.

However, this approach brings disadvantages for all parties involved:

» **Effort for End-User Organizations:** Each module requires a separate integration that the end-user organization must configure and maintain. This process needs to be repeated individually by each organization, leading to significant workload for both the end-user organization and the application developers providing support. The likelihood of errors increases, and synergy effects from customer installations during application development are limited, often restricted to documenting best practices.

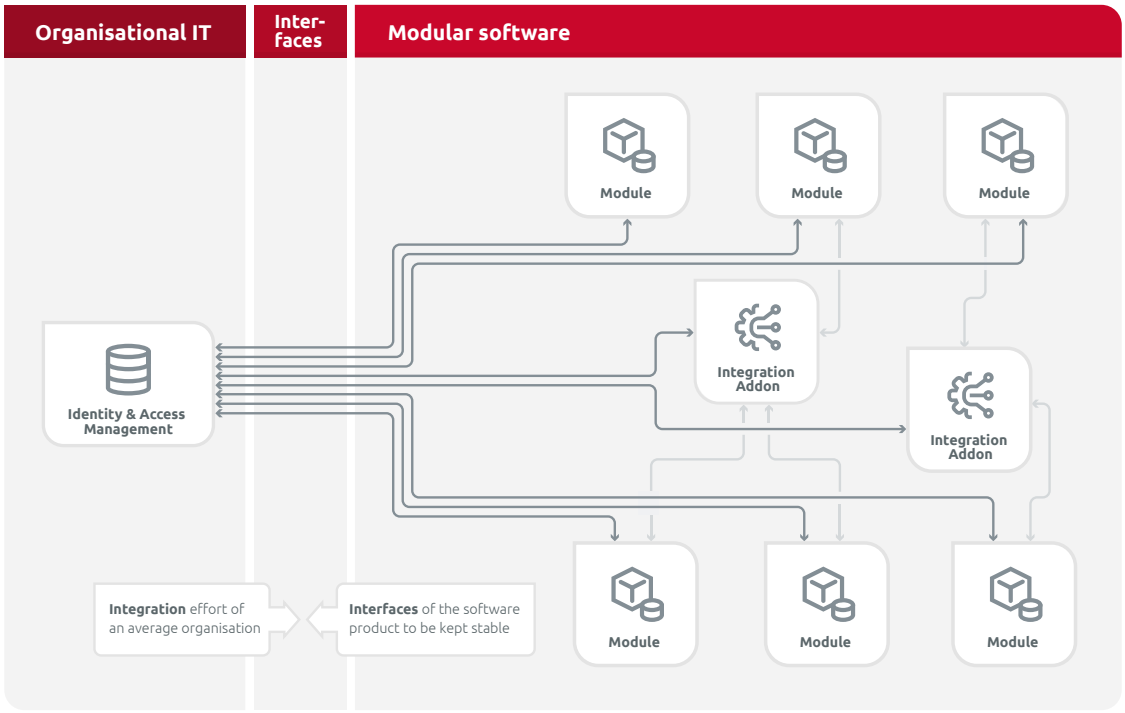


*Figure 1: Integration of a Modular Software Product without IAM Integration into an Organization's IT*

» **Effort and Limitations for Application Developers:** Developers have to document and maintain the interfaces for each module's integration, leading to considerable effort and restricting their flexibility. Any changes to interfaces due to new or updated modules require the involvement of the end-user organization, which often results in changes being avoided, thereby hindering innovation within the modules.

» **Unclear Distribution of Responsibilities:** The individual integration of modules leads to unclear responsibility between the application developers and the end-user organization. A fully functioning application requires correct configuration of all module integrations, taking into account both the IT environment of the user organization and the modules provided by the application developer. Errors in configuration often become apparent only when the modules interact, making them difficult to identify and resolve.

» **Increased Risk of Errors and Security Issues:** The numerous configurations required for module integrations raise the potential for errors, leading to both functional issues for end users and security risks. The complexity and variety of configurations make error analysis significantly more difficult and time-consuming, further increasing the likelihood of undetected issues and vulnerabilities.

The complexity arising from the individual integration of software application modules into existing IT landscapes leads to increased workload for all parties involved, heightened security risks during operation, and ultimately reduces the willingness to adopt new software applications.

## 4. Solution: Implementing a Module for Centralized IAM Integration

The integration of an application into an existing IT landscape should generally adhere to the principle of providing only one interface for a specific purpose. In the case of identities and permissions, which affect multiple modules, a central module should be established within the application to handle IAM integration for the entire system.

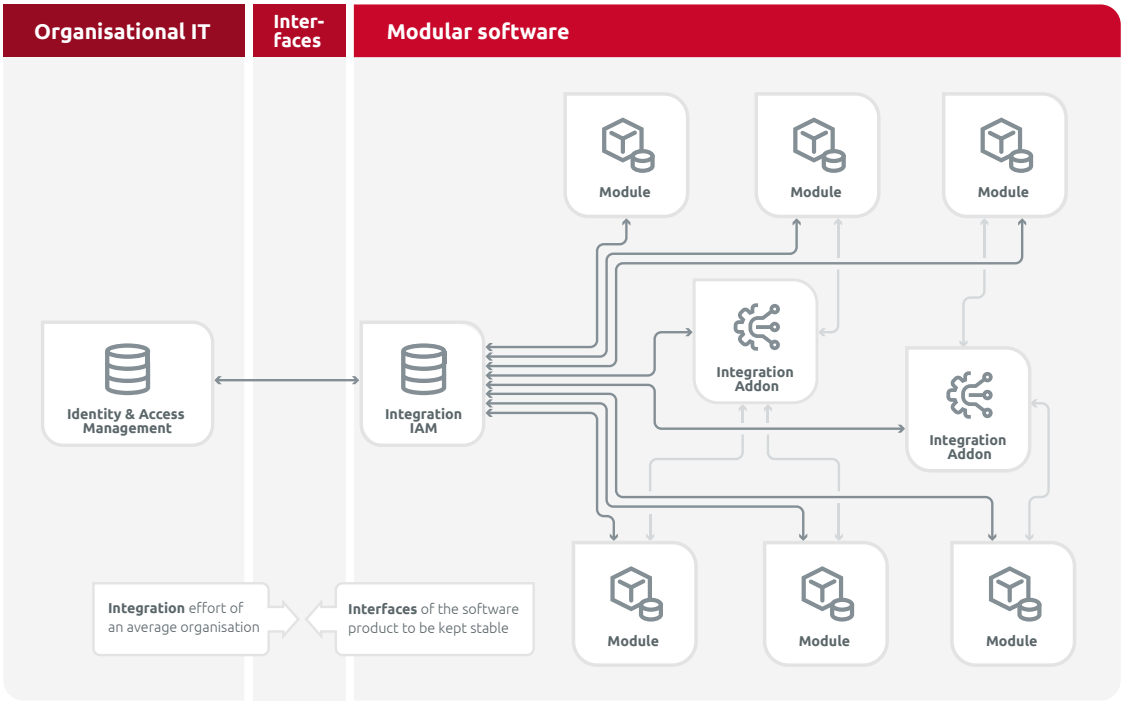


*Figure 2: Integration of a Modular Software Product with IAM into an Organization's IT*

This approach offers several key benefits:

- **Single Integration Point:** The application's modules connect to the organization's IAM system through a single, central IAM module. This significantly reduces the configuration workload for the end-user organization and speeds up the application's deployment.
- **Standardized Integration:** The connection is standardized, making it easier to replicate across different end-user organizations. This reduces the documentation and support workload for application developers.
- **Independent Innovation:** Application developers can introduce or swap out innovations within modules without requiring the end-user organization to alter its existing configurations. New features can be delivered as simple updates.
- **Synergy Effects:** By sharing module integrations with the central IAM module, significant synergy effects are achieved. Improvements in integrations between modules benefit all customers directly, as they are not dependent on the configurations of individual end-user organizations.
- **Clear Responsibilities:** Responsibilities for integrating the software modules into a complete solution are clearly defined and can be managed by the application developers.
- **Simplified Error Analysis:** Using a central IAM module makes it easier to identify and resolve errors. Since all IAM-related requests go through a single interface, isolating the cause of issues and ensuring consistent troubleshooting is significantly more straightforward.

To ensure effective integration of identities and identity structures, it is essential to implement a dedicated IAM integration module within an application. This module provides the necessary interface for connecting to the end-user organization's IAM system and facilitates the integration of individual software modules within the application.

# 5. Using Nubus for IAM Integration


Nubus is an Open Source solution for integrating identity and access management (IAM) across various applications. It combines standard interfaces for IAM, application integration, and user portals, significantly simplifying the implementation, administration, and operation of modular software applications.

Nubus offers comprehensive capabilities for managing users, groups, and their permissions, all supported by a user-friendly web portal. This portal features Single Sign-On (SSO), two-factor authentication, and self-service options, providing end users with secure and straightforward access to all connected services.

The solution uses multiple interfaces to integrate various application modules and offers packaged integrations for well-known and widely-used Open Source applications like Open-Xchange, Nextcloud, Collabora, OpenProject, Xwiki, Jitsi, and Elements.

These integrations are built on Nubus's standard interfaces and can serve as templates for custom application integrations. Nubus can be deployed on Kubernetes or as a component of Univention Corporate Server (UCS) in virtual machines.

Nubus is designed for cloud service providers who want to offer user-friendly SaaS solutions, as well as for IT departments deploying applications within their own organizations. The solution meets common compliance standards, such as BSI IT-Grundschutz conformity and the requirements of the German Administrative Cloud Strategy.

# 6. Case Study: openDesk

openDesk
Der Souveräne Arbeitsplatz

The Sovereign Web Workspace, openDesk, is a web application that combines various Open Source modules into a comprehensive solution, including Univention Nubus for IAM integration. Nearly all modules require IAM integration to securely and user-friendly provide end users with the necessary functions. Additionally, the modules are integrated with each other, for example, allowing files from the cloud storage module (Nextcloud) to be easily accessed through the groupware (OX App Suite) or the project management module (OpenProject). Secure integration of these modules requires them all to be connected to a common IAM system.

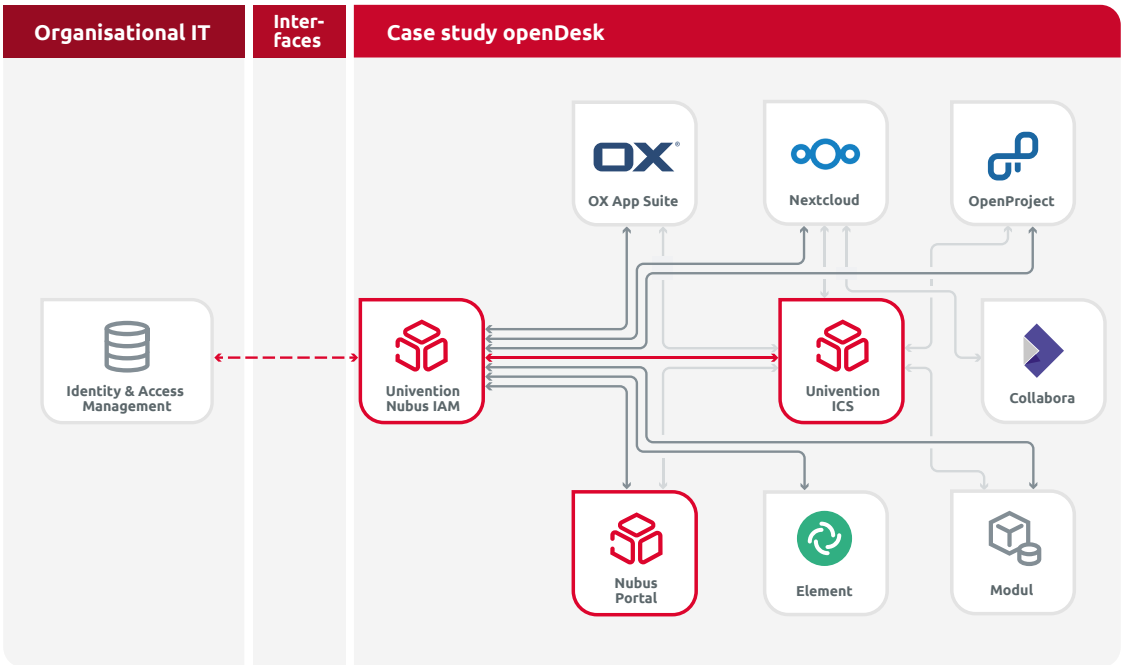


*Figure 3: Case Study openDesk*

Through this approach, openDesk minimizes the effort required by end-user organizations for the implementation and operation of openDesk while ensuring the flexibility to add or replace modules within the platform.

This approach also offers clear advantages for application development within openDesk. Many of the openDesk modules are based on Open Source software that continues to be developed outside of the platform. Thanks to the IAM integration, interfaces for new versions of module software can be updated without needing to modify interfaces in openDesk as a whole. This greatly simplifies the adoption of innovative updates within individual applications and enhances the integration across openDesk modules.

## About Univention

Headquartered in Bremen, Univention offers Open Source solutions for the efficient management of digital identities and application integration. The company focuses on openness, scalability, and ease of use in its products, aiming to ensure digital sovereignty for user organizations. This is achieved by providing control over their own data and identities, as well as enabling the independent design of their IT infrastructure.

Nubus is our central solution for Identity & Access Management, featuring a web portal for easy access to applications and the integration of applications via standardized interfaces and integration packages.

Univention Corporate Server (UCS) is an open integration platform that includes Nubus and its own App Center, enabling the central management of heterogeneous IT domains. UCS can be deployed either as a software appliance in your own data center or in the cloud.

UCS@school is our dedicated solution for the education sector, offering educational authorities an optimized platform. It facilitates the easy deployment of services like learning management systems, email, cloud, and office applications through dedicated school portals. Users can be automatically imported from state directories and centrally managed.

Our solutions are used by numerous federal states, municipalities, counties, administrations, and businesses across the DACH region.

Univention GmbH
Mary-Somerville-Straße 1
28359 Bremen
Fon: +49 (0)421 22232-0

info@univention.de
www.univention.de

univention
be open.