BUSINESS PAPER

Overview

A secure and efficient access to the relevant data is especially important for employees. Therefore, the investment in Identity and Access Management (IAM) has a particularly high priority. For this, not only the use of a corresponding software solution is important, but also the adaptation or modelling of the business processes within this software, which must fit into the existing IT environment. Every company is unique and does not have the time or resources to develop a custom IAM system. For this case, Oxford Computer Group GmbH (OCG) has developed the IAM system "IDABUS".

OCG is a recognized expert in the planning and implementation of IAM systems and has been working in close cooperation with Microsoft for 15 years. IDABUS is therefore positioned as a cloud successor to Microsoft Identity Manger 2016 (MIM).

With IDABUS, uncertainties and costs in the management of identities can be reduced, as security, efficiency and compliance requirements are fulfilled.

IDABUS is used to manage and group identities during their lifecycle within a company. The identity management system can be customized according to different company requirements. Dynamic workflows and processes can be designed to meet company-specific compliance and security requirements.

We have dedicated ourselves to the motto "Performance by Design" during the development. This motto is reflected in all software components. Thanks to the use of Azure resources, both the frontend and the backend are individually and dynamically scalable in order to be able to compensate workload peaks individually.

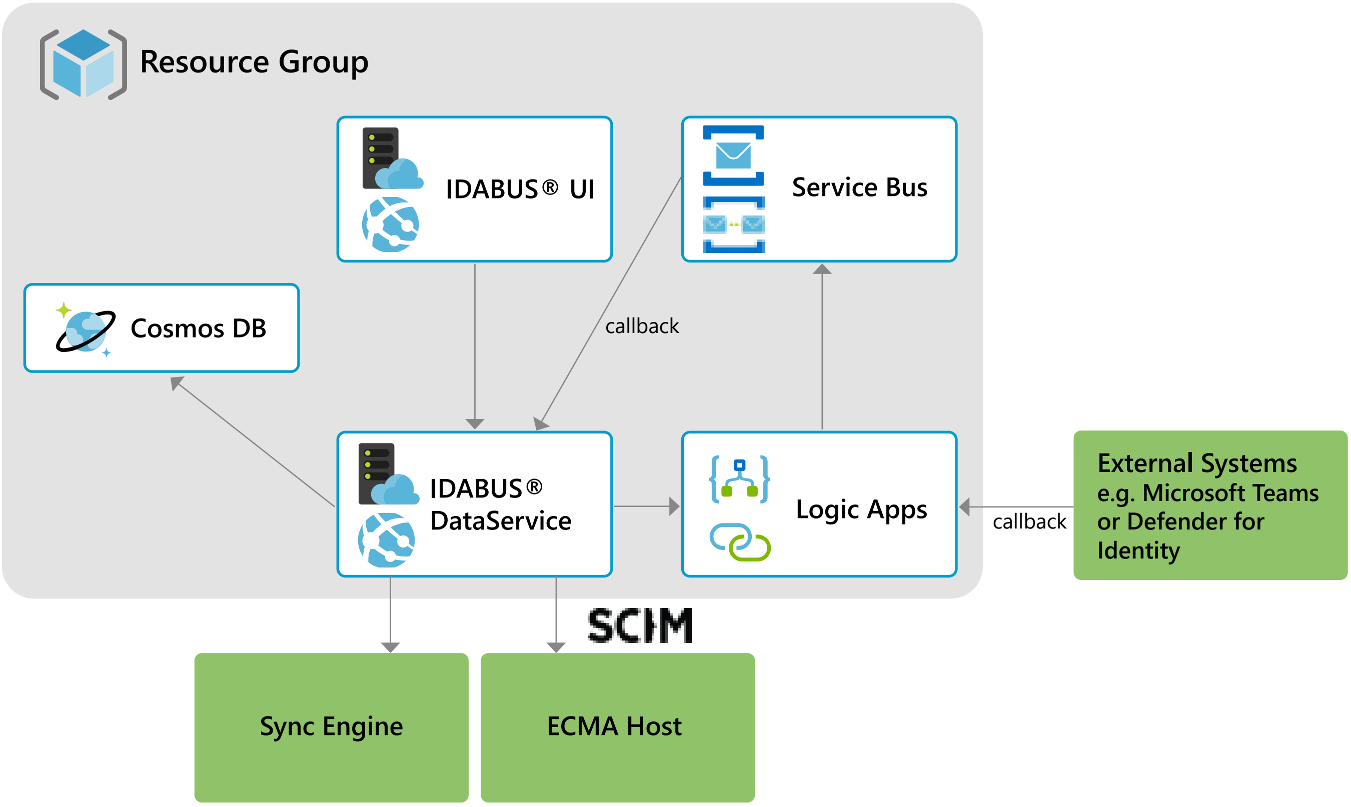
Azure Architecture

IDABUS uses various Azure technologies. The basis is a Cosmos database - a NoSQL database that is characterized by response times in the millisecond range. Another decisive factor in choosing the Cosmos database was its instant scalability, which ensures business continuity even with large data volumes.

Another component is the DataService. It belongs to the backend and is a RESTful API. The DataService covers all basic functions of an IAM system (e.g., creation of object types, attributes, workflows, etc.). The DataService is provided using the Azure App Service. This enables load balancing and automatic scaling according to individual workload peaks. The same applies to the frontend - the IDABUS UI. The user interface offers the possibility to model the company processes and to create and manage identities (users, groups, organizational units, etc.). The IDABUS UI is also provided via the Azure App Service and uses the DataService to save the data in the Cosmos database.

The two other components are the Azure Logic Apps and the Azure Service Bus. By means of the Azure Logic Apps, the DataService is extended by various functionalities, such as the sending of mails, the time-controlled start of a workflow or the asynchronous call of an external API. In the case of an asynchronous call, the Azure Service Bus, which forms the interface to the ‘Callback’ Logic App, takes effect. The Azure Service Bus delivers the response of the external API to the DataService. This behavior has proven to be robust and fail-safe.

Graphic Azure Architecture



Basic Functions

The basic functions of IDABUS correspond to the basic functions of Microsoft Identity Manager 2016. Accordingly, the object and attribute schema used in IDABUS can be extended as desired. These objects and attributes (resources) can be changed as requested via automated workflows. By means of the workflows, the resources can be individually created, changed, and deleted. There are also approval workflows, workflows for e-mail notification (with mail templates), and a time delay for the workflows. Each change or process to a resource remains traceable in the system, i.e., the type of activity, the time of the change and the person executing the change are saved. Furthermore, IDABUS supports an XPath-based query language, which makes it possible to group certain resources according to its properties. IDABUS also enforces data integrity so that no objects or references are orphaned in the system.

Traceability – Object History

The IDABUS object history offers smart reporting for the traceability of the data. This includes a classic overview of all events as well as a visualization of the resource change on the timeline. The display of historical states is calculated in a performant way. In addition, causal relationships can be displayed within the object history. Another special feature is the restoration of historical states. Here, the revert or undo function is used to restore a previous state.

Simulation & Preview

The IDABUS preview function offers the possibility of a preview of the following effects of a change. This makes it possible to estimate the effects in advance, especially in complex contexts. The following effects can be displayed on the one hand by means of a graph and on the other hand by means of a tree view. Furthermore, additional details are available, such as the event type, event status or the requestor. In this view, the user has the option to leave the preview mode and not apply the changes or to leave the preview mode and save the changes.

Advanced Process Management

Extended process management includes the representation of processes by means of a graph. It is particularly important to emphasize that the visualization of the processes shows the causal relationships between users and system processes. Within this graph, it is possible to stop, continue, cancel, or correct individual process steps or workflow executions. When displaying the process graph, there is also the option to completely undo changes including all resulting effects (undo or revert function). The extended process management also includes various workflow activities that go far beyond the basic functionality:

- If-Then-Else workflows: This workflow performs either one or the other activity depending on whether the specified condition returns 'true' or 'false'.
- ForEach workflows: This workflow iterates over a list of values, repeatedly executing a sub-activity.
- Time-based/periodic workflows: This kind of workflow can start independently of a request at a specific time or periodically.
- AddDelay workflows: Any amount of time can be specified here which must expire before the workflow starts. If the delay is greater than 10 seconds, the workflow runs asynchronously, i.e. the workflow event gets the status 'Waiting' and the wait is executed via a Logic App. This means that waiting also works if the server is shut down or restarted in the meantime.
- Approval workflows: This workflow starts an asynchronous approval process with any number of escalation levels.
- RestAPICall workflows: This type of workflow enables arbitrary extensibility and integration of various third-party systems (detailed description in the following section: Extensibility & Integration).

Extensibility & Integration

IDABUS offers an OpenAPI-specified REST interface for extension in order to be able to control third-party systems with it. This extension is realized by means of a workflow that can execute a synchronous or asynchronous REST API call. With the option of an asynchronous call, it is also possible to control external systems whose response request may only arrive with a delay. For this purpose, the http request is set to the status 'Waiting' and waits for a callback.

Another interesting possibility to extend IDABUS is the integration of a Microsoft Teams app. MS Teams is used daily by many companies/organizations and can be used everywhere via the mobile and desktop version. For this reason, IDABUS provides a native Teams app to process self-services (such as applying for group memberships) or administrative IAM tasks (such as approvals or PAM requests). Using the native Teams app is secure and efficient. No separate authentication is required as the single sign-on token is used, and multiple logins are not necessary. With this app, everyday administrative IAM tasks are outsourced to Microsoft Teams, as many users already use Microsoft Teams for their daily work.

Migration

Our top priority was to ensure that existing IAM environments with Microsoft Identity Manager 2016 are not lost in use. Therefore, these environments are subject to investment protection - this means that investments already made, such as the adaptation according to the individual business logic, can be taken over during a migration to IDABUS. This makes the switch to a new IAM system less time-consuming and more expensive.

For the migration, a special tool was developed that converts the data of the MIM. Currently, the following resources can be migrated: users/groups, UI configurations, sets, MPRs, workflows, roles, and the schema. The migration tool is a command line program and takes place in three steps: schema migration, resource migration, system migration. In addition, an import tool is provided for fast loading of large amounts of data.

Training

Oxford Computer Group offers appropriate training for the new IDABUS system. These are divided into UI and System training:

UI Foundation	UI Developer	System Foundation	System Operator
Installation & customizing of the UI	Extension modules for UI	Basic configuration of the system such as workflows, triggers, XPath queries, managed resources	Operation - Installation / Operation / Maintenance / Troubleshooting