IS4U REFERENCE CASE

DIGIPOLIS

IAM / KEYCLOAK

"FASTER, CHEAPER, INNOVATIVE AND FLEXIBLE ICT SOLUTIONS THAT ENABLE PERSONALIZED E-SERVICES..."

ABOUT DIGIPOLIS

A unique city also wants to be the best in the digital world. That is why Antwerp relies on the people of Digipolis for their ICT services.

Digipolis develops software, implements hardware, networks and telephony infrastructures. In addition, they guide their colleagues at Antwerp City, OCMW, Zorgbedrijf Antwerpen and the police, they realize ICT projects and they provide qualitative and stable support for the operational applications and infrastructure.

IS4U

THE CHALLENGE

A flexible and future-proof *Identity and Access Management engine*

IS4U was tasked with **building**, **implementing** and **expanding** the Identity and Access Management Engine. This ensures that the ICT solutions in the Digipolis IT ecosystem have a flexible and future-proof IAM engine.

Digipolis had a number of specific objectives in mind, such as **user registration, authentication levels, delegated role management, authorization for the development platform of the Digipolis IT ecosystem, Single Sign-On (SSO) across all organizations, integration with Apache Kafka and custom login options per organization.**

OUR APPROACH

User Registration

- Users do not need to register themselves, but are automatically added after federation with existing external identity providers.
- An authorization system has been set up for developers who collaborate on an application via the development platform of the Digipolis IT ecosystem. A tailor-made API was made available for this.
- For managing users and groups to simplify integration with other components in the Digipolis IT ecosystem, the implementation of a tailor-made API in Keycloak was realized.

Authentication Levels

- The integration of the 'A-profile login system' has been enabled in Keycloak, so that it can be used as one of the available 'identity providers' in the system.
- Furthermore, a required 'authentication level' was set per application, whereby logging in with a username and password gives a lower level than via ItsMe or eID. The authentication level that can be reached with a login method has also been made adjustable per tenant.
- The expension of Keycloak has the advantage of redirecting users with an authentication level that is too low to the correct authentication mechanism in order to achieve the intended security level. If this cannot be achieved, the user will be refused to login to the desired system. This is known as **Step-Up Authentication**.

Delegated role management

- Each organization can determine for itself what the registration options are.
- Digipolis can delegate the management of the roles/permissions of the applications to the responsible per organization (admins). This allows the organizations, among other things, to determine the roles and rights within their own organization.

Single Sign-On (SSO) across all organizations

- Although **Single Sign-On (SSO)** had to be provided across all organizations (cross-tenant Single Sign-On), Digipolis wanted to segment the users (subset of users per organization). Once a user has authenticated with a particular organization, they do not have to authenticate again, even if it is an application from another organization. Example: I register for an application from Antwerp (as an employee of Antwerp, with my M-profile), then I browse to an application from 'Het stedelijk Onderwijs': I do not have to reauthenticate (unless the application requires a higher authentication level or my session has expired).

Integration with Apache Kafka

- Finally, an integration with Apache Kafka has been set up, which was already in use within Digipolis. User events are propagated to various components of the development platform of the Digipolis IT ecosystem, as well as to other applications.

THE RESULT

Commissioned by Digipolis, IS4U implemented an Identity and Access Management engine for the Digipolis IT ecosystem.

The analysis and architecture of the engine was based on the above requirements, prepared by Digipolis, whereby the implementation of the access manager was set up via high availability clustering.

A high-availability cluster can be seen as a group of computers that support certain server applications (hosts) that work together as one system and guarantee continuous up-time. These 'high availability' clusters are used for traffic distribution, backup and failover.

- **Implementation of the access manager; Keycloak:** To meet all engine requirements, including clustering for high availability.
- **Step-up Authentication:** Expension of Keycloak to allow users to reach the intended level of authentication.
- **API** for managing users and groups to simplify integration with the rest of the Digipolis IT ecosystem.
- **Just-in-time user provisioning** of federated users: based on the information provided to us by the identity providers.
- **Multi-tenancy:** organizations can, among other things, determine the roles and rights within their own organization.
- **Cross tenant Single Sign-On (SSO):** a session set up by one tenant can be used later by another tenant after validation of the achieved authentication level. This way the user does not have to log in every single time, but his existing session can be reused.
- **Integration of Keycloak with Apache Kafka** to which other applications can then subscribe.
- **Setting up federation with ACM** (Flemish digital access management) using OpenID Connect (one time password, SMS & ItsMe)**.**
- **Setting up a federation** with the identity provider of Antwerp (for both A-profile and M-profile).

IN NEED OF AN 'IDENTITY AND ACCESS MANAGEMENT' SOLUTION?

Our experts advise and inspire you for the right tailor-made strategy. With the right strategy and approach, your applications are ready for the future!