# Distributed Authentication Mesh

## A Concept for Declarative Ad Hoc Conversion of Credentials


Student

**Christoph Bühler**


Problem: As more and more applications run in containerized cloud environments, securing their architectures against attackers is an important concern. Applications defend themselves against intrusion with various authentication mechanisms such as OpenID Connect. However, legacy applications that are not updated nor rewritten tend not to support modern security standards. Enabling applications to communicate with legacy (or third-party) software often requires to introduce code changes to the modern apps.

To eliminate leaking credentials (such as access tokens) and to reduce the risk of bugs, this project targets the dynamic conversion of a user identity. This identity is used to authenticate the user instead of the original credentials. This project provides the conceptional idea and the architecture, as well as a platform specific example of such a solution. A Proof of Concept answers relevant questions for the realization of such a framework. The evaluation then shows that the proposed solution is as secure as the current state of the art and validates the architecture against the goals. The conclusion provides information about the project, possible use cases, and the goals of follow-up projects.

Conclusion: This project developed a potential solution to the problem of dynamic credential transformation in systems with diverging authentication mechanisms.

With a brief overview in the introduction, the reader has an overview over the problem and the goal of the project. The definitions explain used technologies and give vital information about security, authentication and Kubernetes.

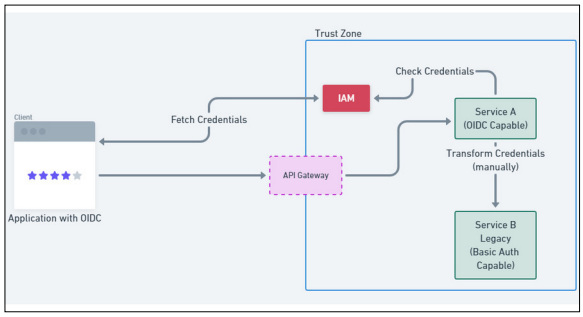
To solve the stated problem, a conceptional architecture is proposed. This architecture contains a "translator" that converts authentication credentials into a common format and vice versa. Furthermore, an optional automation engine enhances applications in a cloud environment with sidecars to integrate them into the authentication mesh. To show the architecture within a practical environment, the project also gives a platform-specific example of the architecture in Kubernetes.

The design of the distributed authentication mesh came close to the concept of SAML (Security Assertion Markup Language). While SAML provides a federated identity, it requires the participating services to implement the SAML protocol as well, the authentication mesh removes this requirement.

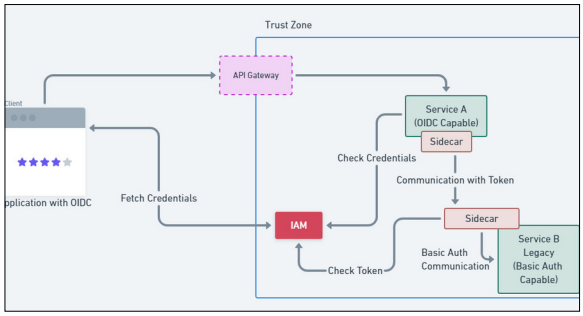
When regarding the current trends, applications will become more heterogeneous in the future. Authentication protocols come and go and it is not likely that one particular standard will solve all issues.

The concepts of this project contribute to sustainability and reusability in the security world.

**Example where the dynamic transformation of credential is useful.**
Own presentment




**Application overview of the Proof of Concept. The sidecars ensure that the target service has the correct credentials.**
Own presentment





Advisor
**Prof. Dr. Olaf Zimmermann**


Subject Area
**Computer Science, Software and Systems**