Title*

Some SubTitle

Christoph Bühler

Autumn Semester 2021
University of Applied Science of Eastern Switzerland (OST)

This is the abstract. TODO.

*I'd like to say thank you :)

Contents

List of Tables

List of Figures

Declaration of Authorship

I, Christoph Bühler, declare that this project report titled, "Distributed Authentication Mesh" and the work presented in it are my own.

I confirm that:

- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. Except for such quotations, this project report is entirely my own work.
- I have acknowledged all main sources of help.
- Where the project report is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Gossau SG, September 27, 2021

Christoph Bühler

1 Introduction

With the introduction of the concept “Distributed Authentication Mesh” [1], a theoretical base for dynamic authorization was created. The project, in conjunction with the Proof of Concept (PoC) showed, that it is generally possible to transform the identity of a user to another application. This transmitted identity can authenticate the user in a trusted system.

This project enhances the concept of the “Distributed Authentication Mesh” by specifying the transport protocol for the common language between services.

The remainder of the report describes prerequisites, used technologies and further concepts.

2 Definitions and Clarification of the Scope

This section provides general information about the project, the context, and prerequisite knowledge. It gives an overview of the context as well as terminology and general definitions.

2.1 Scope of the Project

2.2 Kubernetes and its Patterns

2.2.1 Kubernetes, the Orchestrator

2.2.2 Operator, the Reliability Engineer

2.2.3 A Sidecar, the Extension

2.3 Securing Communication

2.3.1 Basic Authentication (RFC7617)

2.3.2 OpenID Connect (OIDC)

3 The Common Identity Format

This section analyzes different approaches to create a common language format between the service of the "Distributed Authentication Mesh." After the analysis, the definition and implementation of the common format enhances the general concept of the Mesh and enables a production-grade software.

3.1 A Way to Communicate with Integrity

3.1.1 YAML, XML, JSON, and Others

3.1.2 X509 Certificates

3.1.3 JSON Web Tokens

3.2 Implementing a Secure Common Identity

- implement the PKI
- usage of PKI key material
- use key material to sign JWT tokens
- "translator" can validate JWT tokens with key material

4 Limiting Access with Rules

- Create a format / definition for rules that can limit the access to services
- This is “conditional access”
- Create / implement a rule engine that runs as sidecar (like translator)

5 Conclusions and Outlook

Bibliography

[1] C. Bühler, “Distributed authentication mesh,” 2021.

Appendix A - if any

Some Appendix