TODO*

Definition and Implementation of a Common Identity for Secure Transport

Christoph Bühler

Spring and Autumn Semester 2022
University of Applied Science of Eastern Switzerland (OST)

TODO

*I would like to express my appreciation to Mirko Stocker for guiding and reviewing this work. Furthermore, special thanks to Florian Forster, who provided the initial inspiration and technical expertise of the topic.

Contents

List of Figures

Declaration of Authorship

I, Christoph Bühler, declare that this MASTER THESIS titled “TODO” 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 MASTER THESIS is entirely my own work.
- I have acknowledged all main sources of help.
- Where the MASTER THESIS 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, March 7, 2022

Christoph Bühler

1 Introduction

The concept of the "Distributed Authentication Mesh" [1] creates a foundation for dynamic authentication and authorization with diverging authentication schemes. Further, "Common Identities in a Distributed Authentication Mesh" [2] defines and implements the common identity that is transported between services. The mentioned projects show with their respective Proof of Concepts (PoC), that it is possible to authenticate a user and transfer that identity over to other applications that do not share the same authentication mechanism. However, both projects only use one trust zone[1]. While still enabling "zero trust"[2], the projects do not enable true "distribution".

In the current state, applications within the same trust zone can communicate with each other and a potential user only needs to enter his credentials (such as username/password) once. When the user is authenticated, his identity (user ID) is encoded in a JWT for other outgoing calls and the receiving party can validate that the user is already authenticated. Then the receiver uses the transmitted information to encode the identity in the corresponding authentication scheme of the destination [1], [2].

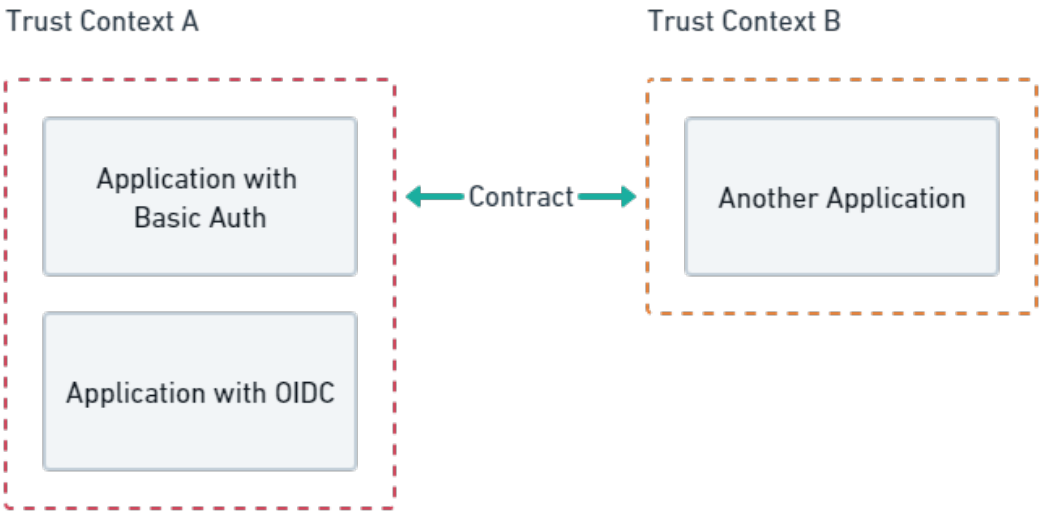

Figure 1: Multiple trust zones that share a contract between them. The contract enables the authentication mesh to verify callers from other zones.

To achieve true distribution, a contract as shown in Figure 1 must exist. The contact defines how multiple parties can trust each other. This project shall define and imple-

[1] A space where applications can "trust" each other.
[2] Assuming that each call can be compromised, so all credentials must be verified for each call.

ment the contract between multiple authentication meshes, such that the distributed authentication mesh can communicate with other trusted zones. To complement the conceptual addition, an open-source implementation of the authentication mesh will be provided. The implementation will run on Kubernetes[3].

The remainder of this thesis describes prerequisite knowledge, used technologies and other topics that are required to understand the work. Section 3 shows the current state of the distributed authentication mesh project and which elements are missing for the true distribution between security contexts. The implementation section, Section 4, provides knowledge about the possible technologies for the contract, defines the contract, and implements the contact along with other implementations needed for the working software. The conclusion then gives an overview of the results and provides an outlook into future work.

[3]https://kubernetes.io

2 Definitions and Clarification of the Scope

This section provides the scope, context and prerequisite knowledge for this project. It also gives an overview of the used technologies as well as an introduction into the security topic of the project. Note that a deeper introduction into other security related technologies is given in the implementation section.

2.1 Scope of this Project

This project builds upon the two former projects "Distributed Authentication Mesh" [1] and "Common Identities in a Distributed Authentication Mesh" [2]. The past work did define a general concept for a distributed authentication [1] and the definition and implementation of a common identity that is shared between the applications in the mesh [2].

The goal of this project is to achieve a distributed mesh. To reach a distributed state in the mesh and to be able to trust other trust zones, a contract between each zone must exist. This project defines and implements the contract and provides the tools that are necessary to run such a mesh in Kubernetes. In this project, we analyze different options to actually form a contract between distant parties and define the specific properties of the contract. After the analyzation and definition, an open-source implementation shall show the feasibility and the usability of the distributed authentication mesh.

Service mesh functionality, such as service discovery even for distant services, is not part of the authentication mesh nor of this project. While the authentication mesh is able to run alongside with a service mesh, it must not interfere with the resolution of the communication. The applications that are part of the mesh must be able to respect the `HTTP_PROXY` and `HTTPS_PROXY` variables, since the Kubernetes Operator will inject those variables into the application. This technique allows the mesh to configure a local sidecar as the proxy for the application.

2.2 Kubernetes

2.2.1 Basic Terminology

2.2.2 What is an Operator

2.2.3 What is a Sidecar

2.3 Trust Zones and Secure Communication

2.3.1 Trust is Important

2.3.2 Zones and Zero Trust

2.3.3 Securing Communication between Parties

3 State of the Art

4 Creating a Trust Context for the Authentication Mesh

4.1 Sign a Contract between Participants

4.1.1 Using a Block Chain

4.1.1.1 Introduction

4.1.2 Using a Master Key

4.1.3 Distribute Contracts via Git

4.2 Define the Contract

5 Conclusions and Outlook

Bibliography

[1] C. Bühler, "Distributed Authentication Mesh - A Concept for Declarative Ad Hoc Conversion of Credentials," University of Applied Science of Eastern Switzerland (OST), Aug. 2021. Available: https://buehler.github.io/mse-project-thesis-1/report.pdf

[2] C. Bühler, "Common Identities in a Distributed Authentication Mesh - Definition and Implementation of a Common Identity for Secure Transport," University of Applied Science of Eastern Switzerland (OST), Feb. 2022. Available: https://buehler.github.io/mse-project-thesis-2/report.pdf