Authorization system description (SysD)

**Abstract**

This document describes the Authorization core system of the Eclipse Arrowhead Framework. The Authorization system is responsible for authorizing interaction between systems in an Arrowhead local cloud in both a centralized and a delegated way.

Table of Contents

[Table of Contents 2](#_Toc106889630)

[1. Overview 3](#_Toc106889631)

[1.1. Significant prior art 3](#_Toc106889632)

[1.2. How this system is meant to be used 3](#_Toc106889633)

[1.3. System functionalities and properties 4](#_Toc106889634)

[1.4. Important delimitations 4](#_Toc106889635)

[2. Services 4](#_Toc106889636)

[2.1. Produced services 5](#_Toc106889637)

[2.2. Consumed services 5](#_Toc106889638)

[3. Security 5](#_Toc106889639)

[3.1. Security Model 5](#_Toc106889640)

[4. Revision history 5](#_Toc106889641)

[4.1. Amendments 5](#_Toc106889642)

[4.2. Quality Assurance 6](#_Toc106889643)

1. Overview

This document describes the Authorization core system, which provides centralized and delegated authorization and management capabilities of the authorization.

The rest of this document is organized as follows. In Section 1.1, we reference major prior art capabilities of the system. In Section 1.2, we describe the intended usage of the system. In Section 1.3, we describe fundamental properties provided by the system. In Section 1.4, we describe de-limitations of capabilities of the system. In Section 2, we describe the abstract service functions consumed or produced by the system. In Section 3, we describe the security capabilities of the system.

# Significant prior art

This system description is derived from the Authorization systems used in version 4 of the Arrowhead Framework and studies of existing off-the-shelf authorization systems.

# How this system is meant to be used

The authorization core system is a system that allows an administrator of an Arrowhead Local Cloud to manage authorization of interaction between different systems in the cloud in a central place. In turn, it allows systems in the local cloud to authorize access to its provided services. This can be done in a centralized way and a delegated way. In the following diagram the interactions and what role the authorization system plays for registration, management and delegated authorization are shown.

A picture containing diagram

Description automatically generated

# System functionalities and properties

The system offers three different functionalities. First, it offers a way to control whether a system is allowed to interact with a provided service of another system. This is done via the Authorization Control service. This can be used by either the consuming system to pre-emptively ensure it is allowed to call the service or by the service provider to authorize an inbound request.

Second, the system offers a way for two systems to authorize requests between each other without the authorization system being a synchronous dependency in the critical request path. This is done using proof-of-access obtained and verified via the Delegated Authorization service.

Finally, the system offers a service to manage the underlying authorization rules used by the two previous services. This service, Authorization Management, would be used by an administrator, which could be either a system (e.g., an administration UI) or a person directly interacting with the service.

# Important delimitations

This document describes the authorization system as a separate system. However, in practise, authorization capabilities are typically combined with authentication and audit. While this is an option this document makes no such assumption, and the authorization system must be able to work independently.

1. Services

The Authorization system should produce services to perform authorization in a centralized (Authorization Control) and a delegated (Delegated Authorization) way as well to manage the authorization rules (Authorization Management). For the Authorization system to advertise its existence in the local cloud, the system registers itself in the service registry using the service discovery service.

A picture containing timeline

Description automatically generated

# Produced services

The Authorization system produces the following services:

|  |  |
| --- | --- |
| Service name | SD |
| Authorization Control | SD Authorization Control |
| Delegated Authorization | SD Delegated Authorization |
| Authorization Management | SD Authorization Management |

# Consumed services

The Authorization system consumes the following services:

|  |  |
| --- | --- |
| Service name | SD |
| Service Discovery | SD Service Discovery |

1. Security

# Security Model

A concrete implementation of the Authorization system may require authentication for the authorization control and delegated authorization services, for specifics refer to each Service Description (SD) and Interface Design Description (IDD).

The authorization management service should be protected by authentication to avoid undesired changes to the underlying authorization rules. Depending on the implementing system this could be, for example but not limited to, X.509 certificates, Bearer tokens or Basic authentication.

Finally, the data stored by the system should be encrypted at rest to avoid any tampering with the data outside of the running application.

1. Revision history

# Amendments

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Date | Version | Subject of Amendments | Author |
| 1 | 2022-06-23 | 1.0 | First draft version for AH 5.0. | David Rutqvist |
| 2 |  |  |  |  |

# Quality Assurance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Date | Version | Approved by |
| 1 |  |  |  |
| 2 |  |  |  |