Authorization HTTP/TLS/JSON

System Description

Abstract

This document describes the Authorization core system of the Eclipse Arrowhead Framework. This core system takes responsibility for authorizing interactions between systems and generating the necessary access tokens.

ARTEMIS Innovation Pilot Project: Arrowhead
THEME [SP1-JTI-ARTEMIS-2012-AIPP4 SP1-JTI-ARTEMIS-2012-AIPP6]
[Production and Energy System Automation Intelligent-Built environment and urban infrastructure for sustainable and friendly cities]

Contents

1 Overview

This document describes the HTTP/TLS/JSON Authorization Eclipse Arrowhead system, which exists to limit access between systems via Authorization Rules in a Eclipse Arrowhead Local Cloud (LC). Examples of such interactions is a consumer system (Consumer A) that would like to consume a given service (Service A), this service is offered by multiple providers (Provider A, ..., Provider N). The preset Authorization Rules define that Consumer A can only access Service A provided by Provider System A, thus it can not access the same service from other providers. This is a whitelist access policy.

This Core System provides a database, it describes which Application System can consume what Services from which Application Systems (Intra-Cloud access rules) also it describes which other Local Clouds are allowed to consume what Services from this Cloud (Inter-Cloud authorization rules).

The purpose of this System is therefore to allow:

- Provide Authorization Control Service (both intra- and inter-Cloud).
- Provide a Token Generation Service for allowing session control within the Local Cloud.

The purpose of the Token Generation functionality is to create session control functionality through the Core Sytems. The output is JSON Web Token that validates the Service Consumer system when it will try to access the Service from another Application System (Service Provider). This Token shall be primarily generated during the orchestration process and only released to the Service Consumer when all affected Core Systems are notified and agreed to the to-be-established Service connection.

This System (in line with all core Systems) utilizes the X.509 certificate Common Name naming convention in order to work.

2 System Role

This System provides two Core Service the **Authorization Control** and **Token Generation** and a utility **Get Public key** service. The first two services are private, thus accessible only by other Core Systems.

There are two use case scenarios connected to the Authorization Core System.

- Check access rights (invokes the Authorization Control)
- Generate an access token (the Orchestrator invokes the Token Generation)

Authorization Control enables to check whether the requested consumer system is allowed to consume the given service by the specified provider.

Token Generation generates a JSON Web Token (JWT) for the client, to enable accessing the requested service.

3 Services

3.1 Consumed Services

3.1.1 Service Discovery Query

This service is consumed in order to look up systems and services in the Service Registry, to determine their availability.

3.2 Provided Services

3.2.1 Token Generation

This service generates a JWT for a client

3.2.2 Authorization Control

This service enables checking whether the requested consumer system is allowed to consume the given service by the specified provider.

3.2.3 Get Public Key

This service provides a public key to requesting system.

4 Security

This System can be secured via the HTTPS protocol. If it is started in secure mode, it enables wider variety of authorization methods:

- Token
- Certificate

5 Revision History

5.1 Amendments

No.	Date	Version	Subject of Amendments	Author
1	2020-12-05	4.3.0		Tanyi Szvetlin
2	2021-01-26	4.3.0	Minor update	Jerker Delsing

5.2 Quality Assurance

No.	Date	Version	Approved by
1	2021-01-26	4.3.0	Jerker Delsing