Authorization

System Design Description

Abstract
This document describes the Authorization core system of the Eclipse Arrowhead Framework. This core system takes responsibility for managing the offered services of all systems.

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

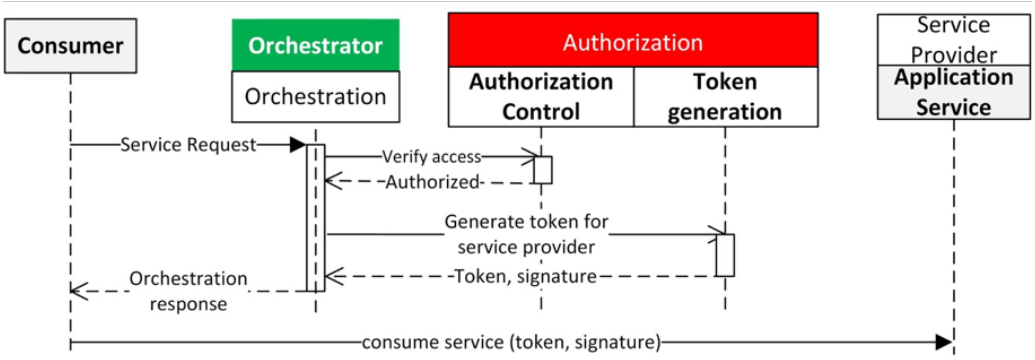

Figure 1: Authorization crosscheck during orchestration process. v4.3.0 only support HTTP/JSON/TLS.

1 Overview

This document describes the Eclipse Arrowhead Authorization system, which exists to manage and to authorize connection between various systems using Authorization Rules in a Eclipse Arrowhead Local Cloud (LC). Examples of such interactions is a consumer system is allowed to consume some kind of Eclipse Arrowhead service offered by an other systems in the LC, because a previously set Authorization Rule enables it.

This Core System provides a database, which stores information related to the currently actively enforced Authorization Rules within the Local Cloud.

The purpose of this System is therefore to allow:

- Provide AuthorizationControl Service (both intra- and inter-Cloud).
- Provide a TokenGeneration Service for allowing session control within the Local Cloud.

The purpose of the TokenGeneration 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.

The v4.3.0 only supports the HTTP protocol, JSON encoding and TLS payload protection.

2 System Role

This System only provides two Core Service the **AuthorizationControl** and **TokenGeneration**.

There are two use case scenarios connected to the Service Registry.

- Check access rights (invoke the AuthorizationControl).
- Generate an access token (the Orchestrator invokes the TokenGeneration).

The AuthorizationControl Service provides 2 different interfaces to look up authorization rights:

- Intra-Cloud authorization: defines an authorization right between a consumer and provider system in the same Local Cloud for a specific Service.
- Inter-Cloud authorization: defines an authorization right for an external Cloud to consume a specific Service from the Local Cloud.

3 Services

3.1 Consumed Services

3.1.1 ServiceDiscovery

This service is provided to allow other systems to **Register** and to **Unregister** their services, and to **Query** public services. In addition the service can Echo that its alive.

3.2 Provided Services

3.2.1 AuthorizationControl

This service is provided to allow the Orchestrator to check whether the requester is allowed to access the requested service.

3.2.2 TokenGeneration

This service is provided to allow access token generation for a consumer system.

4 Security

This System can be secured via the HTTPS protocol. If it is started in secure mode, it verifies whether the Application System possesses a proper X.509 identity certificate and whether that certificate is Arrowhead compliant in its' making. This certificate structure and creation guidelines ensure:

- Application System is properly bootstrapped into the Local Cloud
- The Application System indeed belongs to this Local Cloud
- The Application System then automatically has the right to register its Services in the Registry.

If these criteria are met, the Application System's registration or removal message is processed. An Application System can only delete or alter entries that contain the Application System as the Service Provider in the entry.

5 Revision History

5.1 Amendments

No.	Date	Version	Subject of Amendments	Author
1	2020-12-05	4.3.0		Tanyi Szvetlin

5.2 Quality Assurance

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