Authorization Core System

System Description

Abstract
This document provides system description for the **Authorization Core System**.

Contents

1 Overview

This document describes the Authorization Core System, which exists to manage and to authorize connection between various systems using Authorization Rules within an Eclipse Arrowhead Local Cloud (LC).

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 delimitations of capabilities of the system. In Section 2, we describe the abstract service operations produced by the system. In Section 3, we describe the security capabilities of the system.

1.1 Significant Prior Art

The strong development on cloud technology and various requirements for digitisation and automation has led to the concept of Local Clouds (LC).

"The concept takes the view that specific geographically local automation tasks should be encapsulated and protected." [1]

One of the main building blocks when realizing such Local Cloud is the capability of authorization and session control within the given LC.

1.2 How This System Is Meant to Be Used

Authorization is a mandatory core system of Eclipse Arrowhead LC and is responsible for the fundamental authorization control functionality by storing applicable authorization rules. An intracloud rule describes an access policy between a consumer system and a provider system for a given service, interface pair, while an intercloud rule describes an access policy between a provider system and a neighbor cloud.

This core system is also responsible for providing the session control functionality which is achieved by providing a token generation service.

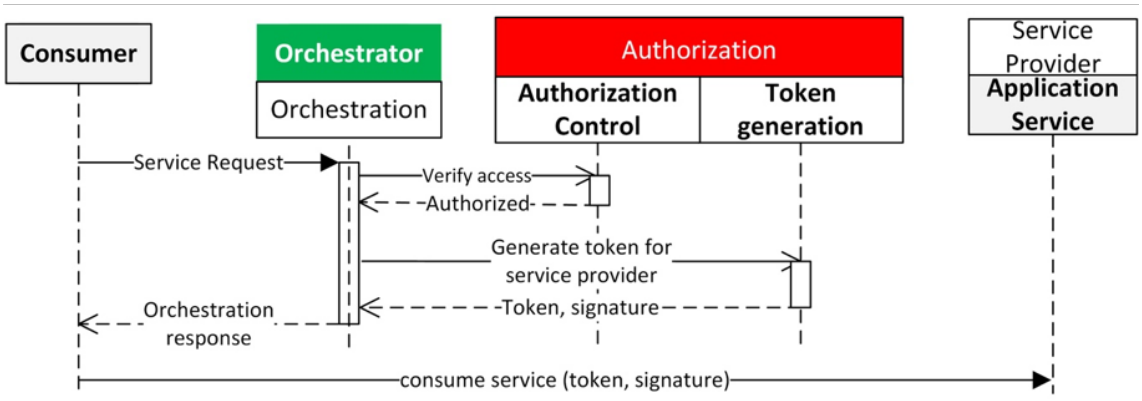

Figure 1: Authorization crosscheck during orchestration process

1.3 System functionalities and properties

1.3.1 Functional properties of the system

Authorization solves the following needs to fulfill the requirements of authorization and session control.

- Enables the system operators to manually create and remove authorization rules.
- Enables the Orchestrator Core system to query the authorization rules during the orchestration process.
- Enables the Event Handler Core system to query the authorization rules during the subscription process.
- Enables the Orchestrator Core system to generate access tokens to the orchestrated provider, service and interface, when it is required.
- Enables the Choreographer Core system to re-generate tokens for executor systems.
- Enables the provider systems to get its public key in order to validate the token received from a consumer.

1.3.2 Non functional properties of the system

Beside the requirements of authorization and session control the Authorization Core System implements certain authentication of systems, meaning that the Authorization makes decision whether a given system has right to use its services or not.

1.3.3 Data stored by the system

In order to achieve the mentioned functionalities, Authorization is capable to store the information set described by figure 2.

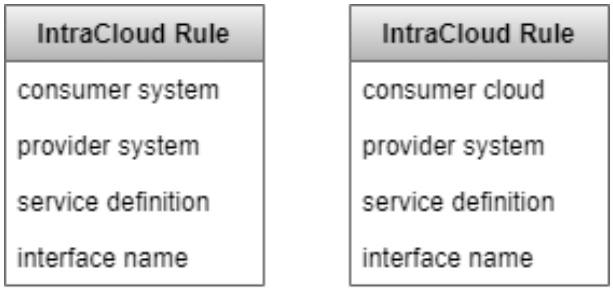

Figure 2: Overview of data stored by Authorization Core System.

1.4 Important Delimitations

While Authorization Core System is responsible for applying the authorization rules, the rules itself can't be generated from higher level policies. System operators always have to define them on system, service definition and interface (database) record level.

Also, the Authorization Core System can't operate without a running Service Registry Core System instances and the access token generation is only possible when the system is running in secure mode.

2 Services produced

2.1 service echo

The purpose of this service is to test the system availability. The service is offered for both application and core systems.

2.2 service authorization-control-intra

The purpose of this service is to query for existing authorization rules for a specified consumer to a specified service definition with possible providers and interfaces. The service is offered only for specified core systems.

2.3 service authorization-control-inter

The purpose of this service is to query for existing authorization rules for a specified consumer cloud to a specified service definition with possible providers and interfaces. The service is offered only for specified core systems.

2.4 service authorization-control-subscription

The purpose of this service is to query for at least one existing authorization rule for a specified consumer to the specified providers. The service is offered only for specified core systems.

2.5 service token-generation

The purpose of this service is to generate access tokens for a consumer to a provider with the content of service consumption session related data. The service is offered only for specified core systems.

2.6 service token-generation-multi-service

The purpose of this service is to execute the *token-generation* service, but for multiple consumers at once. The service is offered only for specified core systems.

2.7 service auth-public-key

The purpose of this service is to provide the public key of the Authorization Core System. It is necessary for validating an access token generated by the Authorization. The service is offered for both application and core systems.

3 Security

The security of Eclipse Arrowhead - and therefore the security of Authorization - is relying on X.509 certificate trust chains. The Arrowhead trust chain consists of three level:

- Master certificate: `arrowhead.eu`
- Cloud certificate: `my-cloud.my-company.arrowhead.eu`
- Client certificate: `my-client.my-cloud.my-company.arrowhead.eu`

For Arrowhead certificate profile see `https://github.com/eclipse-arrowhead/documentation`

4 References

[1] J. Delsing and P. Varga, *Local automation clouds*. Boca Raton: Taylor & Francis Group, 2017, p. 28. [Online]. Available: https://doi.org/10.1201/9781315367897

5 Revision History

5.1 Amendments

No.	Date	Version	Subject of Amendments	Author
1	YYYY-MM-DD	4.6.0		Xxx Yyy

5.2 Quality Assurance

No.	Date	Version	Approved by
1	YYYY-MM-DD	4.6.0	