

Gateway Core System

System Description

Abstract

This document provides system description for the **Gateway Core System**.

Contents

1 Overview	3
1.1 Significant Prior Art	3
1.2 How This System Is Meant to Be Used	3
1.3 System functionalities and properties	4
1.4 Important Delimitations	4
2 Services produced	5
2.1 service <code>echo</code>	5
2.2 service <code>gw-public-key</code>	5
2.3 service <code>gw-connect-consumer</code>	5
2.4 service <code>gw-connect-provider</code>	5
2.5 service <code>gw-close-sessions</code>	5
3 Security	6
4 References	7
5 Revision History	8
5.1 Amendments	8
5.2 Quality Assurance	8

1 Overview

This document describes the Gateway Core System, which exists to establish a secure connection between a consumer and a provider located in different clouds. The concept of the Gateway is described by figure 1.

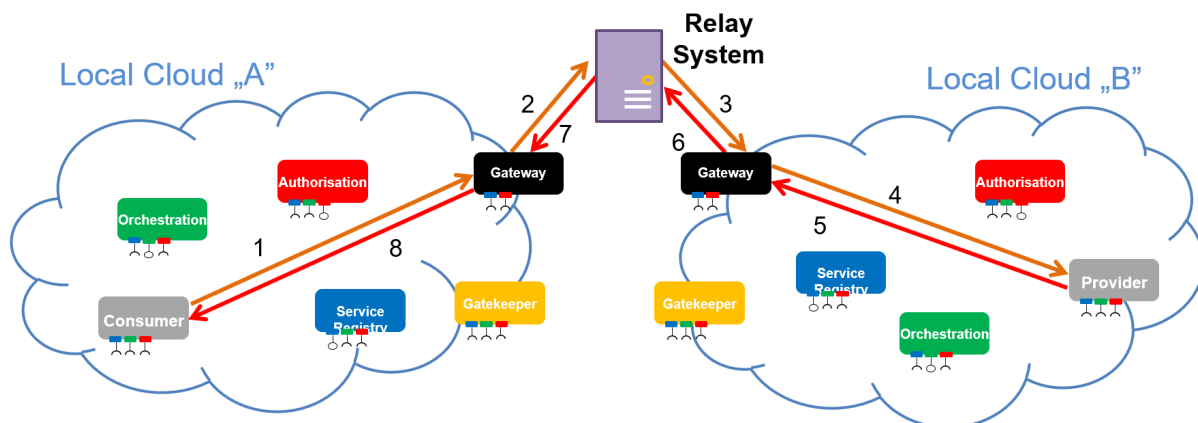


Figure 1: Overview of the Gateway Core System.

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]

Encapsulated and protected LCs means that when a consumer has to use a provider from an other cloud there is no easy way to do that. A gateway support system is needed to create a tunnel between the two application systems on which they can communicate each other without risking their cloud's security.

1.2 How This System Is Meant to Be Used

Gateway is a support core system of Eclipse Arrowhead LC and is responsible for providing secure communication channel between service consumers and providers that are in different clouds.

The building of the secure channel is initiated by the two Gatekeeper Core Systems (one for each participating clouds) during the inter-cloud negotiation process. From an application system's point of view this happens automatically when a consumer can only find matching provider in an other cloud (and those clouds does not support direct access).

1.3 System functionalities and properties

1.3.1 Functional properties of the system

Gateway solves the following needs to fulfill the requirements of providing secure communication channels between clouds.

- Enables the Gatekeeper core systems to establish a connection between the consumer and the provider through cloud boundaries.
- Enables the Gatekeeper core system to get its public key in order to ensure the connection security between the clouds.
- Enables the Workflow Choreographer core system to close unused gateway tunnels.

1.3.2 Non functional properties of the system

The Gateway implements certain authentication capabilities, meaning that Gateway makes decision whether a given system has right to use its services (i.e. only the Gatekeeper can initiate a gateway tunnel creation).

1.3.3 Data stored by the system

The Gateway Core System does not need any persistent storage.

1.4 Important Delimitations

The Gateway Core System can only run in secure mode.

Also, it needs at least one external relay application that is accessible from both participating clouds to enable the communication between application systems of the clouds. Furthermore, the Gatekeeper Core System is also needed to initiate the Gateway's tunnel creation operation.

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 **gw-public-key**

The purpose of this service is to provide the public key of the Gateway Core System. It is necessary to ensure the secure communication between the Gateways.

2.3 service **gw-connect-consumer**

The purpose of this service is to create an access point for the consumer to consume a specific service beyond the cloud boundaries.

2.4 service **gw-connect-provider**

The purpose of this service is to create a proxy that can consume a specific provider of the cloud in the name of a consumer beyond the cloud boundaries.

2.5 service **gw-close-sessions**

The purpose of this service is to destroys the specified gateway tunnels and release their resources.

3 Security

The security of Eclipse Arrowhead - and therefore the security of Gateway - 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>



ARROWHEAD

Document title
Gateway Core System
Date
2023-03-21

Version
4.6.0
Status
RELEASE
Page
7 (8)

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	