Blacklist Support System

System Description

Abstract
This document provides system description for the **Blacklist Support System**.

Contents

1 Overview

This document describes the Blacklist Support system, which makes it possible to ban systems from the Eclipse Arrowhead Local Cloud (LC), so that their requests will not be served. This system provides storage functionality for the blacklist entries that contain information about the ban for each 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 services 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 digitization 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 centrally and consistently control the blacklist within the given LC, and store who was banned, when and why. The Blacklist Support system was not part of the LC in the previous versions (4.6.x), but it is a recommended Support system in versions 5.0.0 and higher.

1.2 How This System Is Meant to Be Used

Blacklist is a recommended Support system of the Eclipse Arrowhead Local Cloud and is responsible to provide a central blacklist functionality by storing the blacklist entries.

1.3 System functionalities and properties

1.3.1 Functional properties of the system

Blacklist solves the following needs to fulfill the blacklist functionality.

- Enables the application and other Core/Support systems to query the blacklist records that apply to them and are in force.
- Enables the application and other Core/Support systems to check if an arbitrary system is blacklisted.
- Enables administrative Support systems to manage (query, create, remove) the blacklist entries.

1.3.2 Non functional properties of the system

If an Authentication system is present in the Local Cloud, the Blacklist system will use its service(s) to verify a requester system before responding to any request. This verification is skipped when the requester is a system operator, or the request is a lookup for the identity service.

1.3.3 Data stored by the system

In order to achieve the mentioned functionalities, Blacklist is capable to store the following information set:

- **Entry**: the name of the banned system and properties of the ban like reason, start date, expiration date, etc...

1.4 Important Delimitations

- If the Local Cloud does not contain an Authentication system, there is no way for the Blacklist to verify the requester system. In that case, the Blacklist system will consider the authentication data that comes from the requester as valid.

2 Services produced

2.1 service blacklistDiscovery

The purpose of this service is to provide information about the blacklist. This service is offered for both application and Core/Support systems.

2.2 service blacklistManagement

The purpose of this service is to manage (query, create and remove) blacklist entries in bulk. The service is offered for administrative Support systems.

2.3 service monitor

Recommended service. Its purpose is to give information about the provider system. The service is offered for both application and Core/Support systems.

3 Security

For authentication, the Blacklist utilizes an other Core system, the Authentication system's service to verify the identities of the requester systems. If no Authentication system is deployed into the Local Cloud, the Blacklist trusts the requester system self-provided identity.

For authorization, the system uses an other Core system, the ConsumerAuthorization system to decide whether a consumer can use its services or not. If the ConsumerAuthorization Core system is not present in the Local Cloud, then the Blacklist allows for anyone in Local Cloud to use its services. The following service operations can always be used without any authorization rules:

- *blacklistDiscovery* service's *lookup* operation,
- *blacklistDiscovery* service's *check* operation.

The implementation of the Blacklist can decide about the encryption of the connection between the Blacklist and other systems.

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	5.0.0		Xxx Yyy

5.2 Quality Assurance

No.	Date	Version	Approved by
1	YYYY-MM-DD	5.0.0	