Authentication system description (SysD)

**Abstract**

This document describes the Authentication core system, which provides a centralized identity store that enables authentication in the Arrowhead Local Cloud.

Table of Contents

[Table of Contents 2](#_Toc106909195)

[1. Overview 3](#_Toc106909196)

[1.1. Significant prior art 3](#_Toc106909197)

[1.2. How this system is meant to be used 3](#_Toc106909198)

[1.3. System functionalities and properties 3](#_Toc106909199)

[1.4. Important delimitations 3](#_Toc106909200)

[2. Services 3](#_Toc106909201)

[2.1. Produced services 4](#_Toc106909202)

[2.2. Consumed services 4](#_Toc106909203)

[3. Security 4](#_Toc106909204)

[3.1. Security Model 4](#_Toc106909205)

[4. Revision history 4](#_Toc106909206)

[4.1. Amendments 4](#_Toc106909207)

[4.2. Quality Assurance 4](#_Toc106909208)

1. Overview

This document describes the Authentication core system, which provides a centralized identity store that enables authentication in the Arrowhead Local Cloud.

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 de-limitations of capabilities of the system. In Section 2, we describe the abstract service functions consumed or produced by the system. In Section 3, we describe the security capabilities of the system.

# Significant prior art

This system description is derived from studies of existing off-the-shelf authentication systems and well-established industry standards such as SAML, OpenID Connect, Kerberos etc.

# How this system is meant to be used

The authentication system is meant to be used by a system that wants to validate the identity of a service request. Similarly, a system may want to prove its identity to another system and therefore identifies itself with the Authentication system and receives a proof-of-identity in return that can be used when calling other services. Authentication is needed for service-to-service calls but also for end-user interfaces that wants to obtain the identity of the current user.

# System functionalities and properties

The Authentication system provides functionality in three areas:

To manage and query identities along with related information. Related information can be metadata such as contact information, structural relationships such as groups, and claims that can be made about an identity such as roles.

To produce a proof-of-identity that in essence is a claim by the Authentication system about the identity of a subject. These claims include an identity and depending on the implementation, any other claims requested, such as roles held by the subject in the claim. The proof-of-identity typically represents the subject requesting the claim.

To allow a system to validate a proof-of-identity carried by an actor interacting with said system. This functionality could be a direct call to the service, or made offline by use of, for example, public key infrastructure (PKI) in which the proof-of-identity is cryptographically signed.

# Important delimitations

While the use of an authentication system is of little use without an authorization system to implement access control, this document does not specify how these two systems relate to each other. In practice, the link between these systems is the proof-of-identity concept, which is a piece of information produced by the authentication system and in some way consumed (likely indirectly) by an authorization system.

1. Services

The Authentication system should produce a service to allow systems to perform authentication by using the Identity Provider service. The authentication system could also produce an identity management service to, for example, to allow creating new users (identities). To allow other systems in the local cloud to know about the identity services, the system registers itself in the service registry using the service discovery service.

Timeline

Description automatically generated with medium confidence

# Produced services

The Authentication system produces the following services:

|  |  |
| --- | --- |
| Service name | SD |
| Identity Provider | SD Identity Provider |
| Identity Management | SD Identity Management |

# Consumed services

The Authentication system consumes the following services:

|  |  |
| --- | --- |
| Service name | SD |
| Service Discovery | SD Service Discovery |

1. Security

# Security Model

The Authentication system is vital to the overall security of a system-of-systems. In particular the Identity Management service needs to be secured properly, both for modifying data but also querying information such as information classified as Personal Data.

The Authentication system must be configured in accordance with the policies set for the system-of-system with respect to authentication mechanisms (e.g., password policy, multi-factor authentication (MFA), lifetime of proofs-of-identity).

Best practice should be followed for storing and transmitting information related to the repository of identities, such as encrypting information, hashing passwords, fingerprints, and the like.

1. Revision history

# Amendments

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Date | Version | Subject of Amendments | Author |
| 1 | 2022-06-23 | 1.0 | First draft version for AH 5.0. | David Rutqvist |
| 2 |  |  |  |  |

# Quality Assurance

|  |  |  |  |
| --- | --- | --- | --- |
| No. | Date | Version | Approved by |
| 1 |  |  |  |
| 2 |  |  |  |