TokenGeneration M3 SD

**Abstract**

This document defines the TokenGeneration M3 service functionality.

1. Service Overview

This document describes an Arrowhead service, including its interfaces, functions and information model.

The TokenGenerationM3 Service provides a session-control token. This token is generated using the public key of the Service Provider, therefore it is only decryptable by that System. The attached signature verifies that the local Authorization System generated the token and therefore verifies authorization status.

The token is generated using RSA/ECB/PKCS1Padding encryption, while the signature is generated using SHA1 with RSA digest.

The encrypted JSON object contains the following fields:

***{***

***„c”: ”<SystemName>.<CloudName>.<Operator>”,***

***„s”: ”<interface>.<ServiceName>”,***

***„e”: ”<endTimeInEpoch>”***

***}***

Where:

* c: consumer System identifier (first part of the certificate Common Name field)
* s: service identifier
* e: token validity end time, in Unix epoch

1. Abstract Interfaces

This Service provides one functionality.

# Generate

This method is used to generate tokens. It is a simple request-response. When this method is invoked, the Authorization System shall log this event for accountability reasons.

1. Abstract Information Model

This Service uses the generic System and Service description objects and naming convention of G3.2. This Service is a single request-response, and Table 1 and 2 describe the information exchanged.

|  |  |
| --- | --- |
| Field name | Description |
| consumer | ArrowheadSystem that will try to access the Service instance. |
| consumerCloud | The ArrowheadCloud where the consumer System is located. If not defined, the Local Cloud is assumed. |
| providers | List of possible Application Systems that can provide the Service. |
| Service | The ArrowheadService that will be consumed. |
| Duration: int | The duration until the Service exchange can happen. |

Table 1 - TokenGenerationRequest

|  |  |
| --- | --- |
| Field name | Description |
| tokenData | Is a list that contains entries consisting of the followings:   * signature: message digest from the Authorization System * system: ArrowheadSystem object of the Provider * token: the actual token for that Provider – Consumer -Service combination |

Table 2 - TokenGenerationResponse

1. Non-functional Requirements

1. Revision history

# Amendments

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No. | Date | Version | Subject of Amendments | Author |
| 1 | 2017-09-29 | M2 | Initial | Csaba Hegedűs |
| 2 | 2018-02-14 | M3 | Updating document to M3 | Csaba Hegedűs |

# Quality Assurance

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