Document title
auth-public-key
Date
2023-03-01
Author
Tamás Bordi
Contact
tbordi@aitia.ai

Document type
SD
Version
4.6.0
Status
RELEASE
Page
1 (7)

auth-public-key

Service Description

Abstract

This document provides service description for the **auth-public-key** service.

Document title
auth-public-key
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
2 (7)

Contents

Document title
auth-public-key
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
3 (7)

1 Overview

This document describes the **auth-public-key** service, which provides the public key of the system. It is necessary for validating an access token generated by the Authorization Core System.

The rest of this document is organized as follows. In Section 2, we describe the abstract message functions provided by the service. In Section 3, we end the document by presenting the data types used by the mentioned functions.

1.1 How This Service Is Meant to Be Used

The provider systems are recommended to use this service at their start up in order to already have this key when a service consumption request arrives and the access the token need to be validated.

1.2 Important Delimitations

The public key string must be a Base64 encoded JSON string.

1.3 Access policy

Available for anyone within the local cloud.

Document title
auth-public-key
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
4 (7)

2   Service Interface

This section describes the interfaces to the service. The **auth-public-key** service is used to provide the public key of the system.

The following interfaces are available.

2.1   interface HTTP/TLS/JSON () : PublicKey

Profile ype	Type	Version
Transfer protocol	HTTP	1.1
Data encryption	TLS	1.3
Encoding	JSON	RFC 8259 [1]
Compression	N/A	-

Table 1: HTTP/TLS/JSON communication details.

Document title
auth-public-key
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
5 (7)

3   Information Model

Here, all data objects that can be part of the **auth-public-key** service provides to the hosting System are listed in alphabetic order. Note that each subsection, which describes one type of object, begins with the *struct* keyword, which is used to denote a collection of named fields, each with its own data type. As a complement to the explicitly defined types in this section, there is also a list of implicit primitive types in Section 3.2, which are used to represent things like hashes and identifiers.

3.1   struct PublicKey

Base64 encoded JSON String.

3.2   Primitives

Types and structures mentioned throughout this document that are assumed to be available to implementations of this service. The concrete interpretations of each of these types and structures must be provided by any IDD document claiming to implement this service.

Type	Description
String	A chain of characters.

Document title
auth-public-key
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
6 (7)

4   References

[1] T. Bray, "The JavaScript Object Notation (JSON) Data Interchange Format," RFC 8259, Dec. 2017. [Online].
     Available: https://rfc‑editor.org/rfc/rfc8259.txt

Document title
auth-public-key
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
7 (7)

ARROWHEAD

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	