Document title		Document type
auth-public-key HTTP/TLS/JSON		**IDD**
Date		Version
2023-03-01		**4.6.0**
Author		Status
Tamás Bordi		**RELEASE**
Contact		Page
tbordi@aitia.ai		**1 (7)**

auth-public-key HTTP/TLS/JSON

Interface Design Description

Abstract

This document describes a HTTP protocol with TLS payload security and JSON payload encoding variant of the **auth-public-key** service.

Document title
auth-public-key HTTP/TLS/JSON
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
2 (7)

Contents

Document title
auth-public-key HTTP/TLS/JSON
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
3 (7)

1 Overview

This document describes the **auth-public-key** service interface, which provides the public key of the system.. It's implemented using protocol, encoding as stated in the following table:

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

Table 1: Communication and semantics details used for the **auth-public-key** service interface

This document provides the Interface Design Description IDD to the *auth-public-key – Service Description* document. For further details about how this service is meant to be used, please consult that document.

The rest of this document describes how to realize the *auth-public-key* service HTTP/TLS/JSON interface in details.

Document title
auth-public-key HTTP/TLS/JSON
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
4 (7)

ARROWHEAD

2 Interface Description

The service responses with the status code `200 Ok` if called successfully. The error codes are, `401 Unauthorized` if improper client side certificate is provided and `500 Internal Server Error` if Authorization is unavailable.

```
1  POST /authorization/publickey HTTP/1.1
```

Listing 1: An auth-public-key invocation.

```
1  "thisisthebase64publickeyjsonstring"
```

Listing 2: An auth-public-key response.

Document title
auth-public-key HTTP/TLS/JSON
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
5 (7)

3   Data Models

Here, all data objects that can be part of the service calls associated with this service are listed in alphabetic order.

3.1   struct PublicKey

Base64 encoded JSON String.

3.2   Primitives

JSON Type	Description
String	An arbitrary UTF-8 string.

Document title
auth-public-key HTTP/TLS/JSON
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 HTTP/TLS/JSON
Date
2023-03-01

Version
4.6.0
Status
RELEASE
Page
7 (7)

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	Xxx Yyy