

JSON Web Token SL

The 'JSON Web Token SL' library contains a function block for creating a JWT (JSON Web Token) on the controller.

Product description

The 'JSON Web Token SL' library contains a function block for creating a JWT (JSON Web Token) on the controller. For this purpose, the algorithms HS256, HS384, HS512, and RS256 are supported.

The 'JSON Web Token SL' library can create signed JWT according to the standard RFC 7519.

The following algorithms are supported for the signature of JWT:

- HS256
- HS384
- HS512
- RS256

Parameters

Internal memory has to be reserved in order to create a JWT. For this purpose, the amount of reserved memory has to be at least the size of the JWT.

The maximum size can be modified in the Library Manager by means of a parameter list of the library (see *Image 1*).


VAR_GLOBAL CONSTANT Global_Constant					
Name	Type	Inherited from	Address	Initial	Comment
 gc_MaxJWTSize	UINT			2047	Maximum size of JWT. Default 2047 => 2048 Bit long JWT

Image 1: Parameter list of the JWT library

Getting started

1. Create a private key

A private key is required for the asymmetric signature algorithm (RS256). For this purpose, the CODESYS Security Agent has to be installed first.

Afterwards, you can use the Security Screen to create a new certificate on the device. Then the 'Common Name' of the certificate is passed to the JWT library.

2. Download and start the project on the controller

Application JWT

For symmetric signature algorithms (HS256, HS384, HS512):

- Use the input sSecret.
- Leave the inputs sUseCaseName and sCommanName blank.

For asymmetric signature algorithms (RS256):

- Specify the inputs sUseCaseName and sCommanName with the data of the certificate.
- Leave the input sSecret blank.

The following functions can be executed via the visualization.

- Setting of the JWT Header and Payload
- Selection of the algorithm
- Creation of a JWT

The screenshot shows a user interface for a JWT application. On the left, under the 'JWT Input' section, there are two large text input fields labeled 'Header' and 'Payload'. To the right of each field are two circular buttons with colored outlines (green, red, and blue). On the right side, under the 'JWT' section, there is a dropdown menu for 'JWT Algorithm' currently set to 'HS256'. Below this are three text input fields labeled 'Secret:', 'Common Name:', and 'Use Case Name:'. At the bottom right, there is a large text input field for the 'JWT' token. Below this field is an 'Execute:' button with a toggle switch set to '0' and two circular buttons with colored outlines (green, red, and blue).

Visualization of the JWT example

General information

Supplier:

CODESYS GmbH
Memminger Strasse 151
87439 Kempten
Germany

Support:

Technical support is not included with this product. To receive technical support, please purchase a CODESYS Support Ticket.

<https://support.codesys.com>

Item:

JSON Web Token SL

Item number:**Sales/Source of supply:**

CODESYS Store
<https://store.codesys.com>

Included in delivery:

CODESYS Package

System requirements and restrictions

Development system	CODESYS Development System V3.5.15.0
Runtime	CODESYS Control V3.5.15.0
Supported platforms and devices	All
Additional requirements	-
Restrictions	The library can create and sign only JWT. It cannot verify the validity of a JWT.
Licensing	License activation is optional on the CODESYS Key or Soft Key. (The Soft Key is a free component of CODESYS Control.) Licensing by means of the Soft Key is bound to the hardware. Note: Without a license, the software runs for 30 minutes in demo mode.
Required accessories	-

Note: Technical specifications are subject to change. Errors and omissions excepted. The content of the current online version of this document applies.

Creation date: 2023-08-21