

JSON WEB TOKEN (JWT)



Sascha Huwald




Sascha Huwald

Director of Technology @ **OSF**DIGITAL

- Co-Founder of **email360**
- Creator of the SSJS Lib



 /sascha-huwald

What are JWTs?



JSON DATA



CRYPTOGRAPHICALLY
SIGNED



NOT ENCRYPTED



SIMPLE IN NATURE

What is a Cryptographic Signature

I got your contact from a South African health officer in Ghana.

I need to move 1,000 Carats of polished Diamond.

Note, this transaction is 100% risk free and dose not attracts any danger.

H. Kamanda Koroma

This is a signature!!



Create a JWT

Header

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}
```



Payload

```
{  
  "sub": "1234567890",  
  "name": "John Doe",  
  "iat": 1516239022  
}
```



Signature

```
HMACSHA256(  
  base64UrlEncode(header) + "." +  
  base64UrlEncode(payload),  
  your-256-bit-secret  
) ☐ secret base64 encoded
```



Base64Encode

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9
```

.

Base64Encode

```
eyJzdWIiOiIxMjM0NTY3ODkwiwiibmF...
```

+

256 bit Secret

Create a JWT

JWT



Header (base64)

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9

.

Payload (base64)

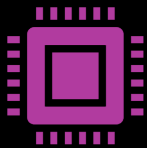
eyJzdWIiOiIxMjMONTY3ODkwIiwibmF...

.

Signature (HMAC)

A6ubTS5mqLu_y0yb6H515e5ZNq2h ...

Definitions



Stateless

A JWT that is entirely self-contained, and holds all user information necessary to complete a transaction



Stateful

A JWT that only contains a session ID or user identifier (SubscriberKey). All user data is stored server-side and need to be retrieved



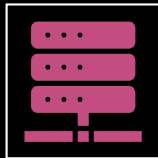
Claims

Claims are statements about an entity (typically, the user) and additional data. There are three types of claims: *registered*, *public*, and *private* claims.

What can we use JWT for?



Prove that some JSON data
can be trusted



Server-to-server integrations
with short EXP claim



API authentication



SFMC – customer access to
Cloudpages



marketing cloud

SFMC REST API

ev.JhbGciOiJIUzI1NiIsInR0eSI6ImtpZCJlOjQ..... ey.JhY2Nlc3NfdG9rZW4iOiI2WnpaZVcyc2I5VHZSRDhycEtkUTJU MzkiLCJjb..... Jdm RdEbZPzCSjtS9OI48E25rvsqxulyD92Xd4mP6ZE....



```
{
  "alg": "HS256",
  "kid": "4",
  "ver": "1",
  "typ": "JWT"
}
```

```
{
  "access_token": "6ZzZeW2wmyTvRD8rpKdQ2T49",
  "client_id": "knfojh0gh9zfya0vfrQz6tq",
  "eid": "5328912",
  "stack_key": "S6",
  "platform_version": 2,
  "client_type": "ServerToServer"
}
```

Signature

JWT in AMP Script is here!

GetJWT

GetJWTByKeyName

```
1 string GetJWT(string key, string algorithm, string jsonPayload)
```

```
SET @JWT = GetJWTByKeyName("INT_SECRET", "HS256", @JSON)
```

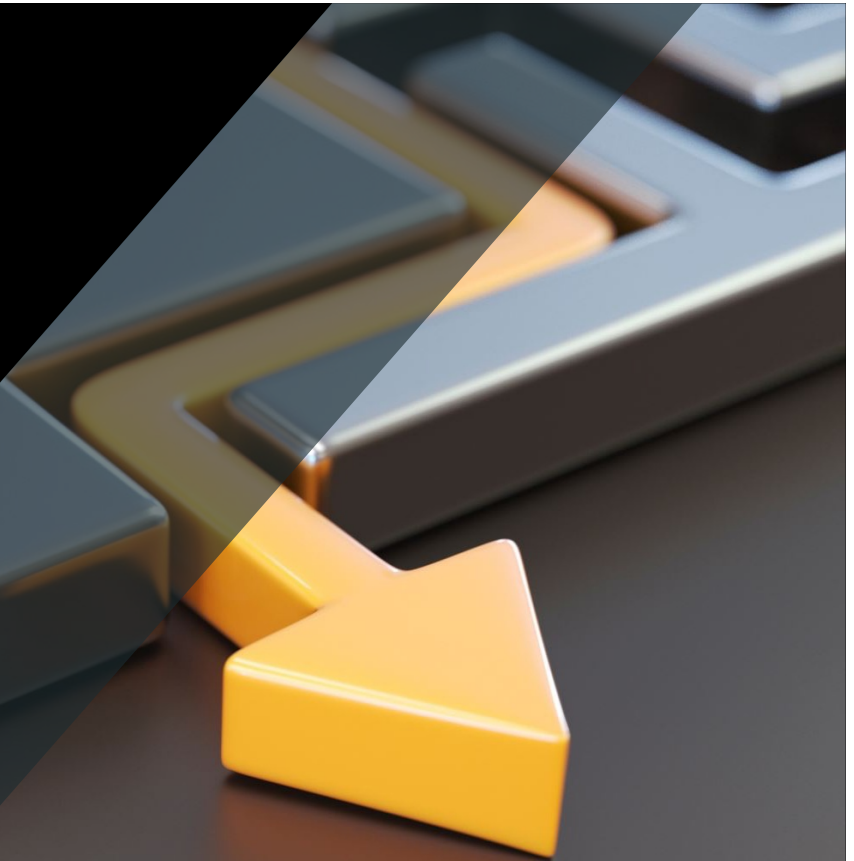


```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjMONTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Only the beginning

No easy way

- ... to decode a token
- ... to add EXP and NBF claims
- ... to verify a token
- ... to sign a token





LIVE DEMO

SSJS here to help