<CodingSonata />

Your Quick Guide to JWT

Aram Tchekrekjian

@AramT87

What is JWT

JWT is short for JSON Web Tokens

It is a standard format to transmit data between systems in a secure way through JSON objects

Why Use JWT?

Authentication

Verifies user identity

Authorization

Grants access to protected resources according to role (in claims)

Stateless

No need to store session data on the server.

@AramT87

JWT Security Model

JWTs are digitally signed to ensure integrity and authenticity

Digital signing ensures no one has tampered with the data contained within the JWT

Optionally, JWTs can also be encrypted to protect sensitive data

@AramT87

JWT Structure

A JWT consists of three parts, each part represented as a base64 URL-encoded string, separated by dots (.):

Header

Contains metadata (algorithm & token type).

Payload

Holds user data (claims).

Signature

Ensures token integrity and authenticity

@AramT87

JWT Example

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJuYW1laWQiOiIxIiwibmJmIjoxNzQxMzI3NjEyL
CJleHAiOjE3NDEzMjg1MTAsImlhdCI6MTc0MTMy
NzYxMiwiaXNzIjoiaHR0cDovL2NvZGluZ3NvbmF
0YS5jb20iLCJhdWQiOiJodHRwOi8vY29kaW5nc2
9uYXRhLmNvbSJ9.
MLzdiWUCEbInTH5YKRpqMmtQ4ptxeMM9LRIjE
a80UCY
```

@AramT87

JWT Example Breakdown

Header

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9

Payload

eyJuYW1laWQiOiIxIiwibmJmIjoxNzQxMzI3NjEyLCJleHAiO
jE3NDEzMjg1MTAsImlhdCI6MTc0MTMyNzYxMiwiaXNzIj
oiaHR0cDovL2NvZGluZ3NvbmF0YS5jb20iLCJhdWQiOiJo
dHRwOi8vY29kaW5nc29uYXRhLmNvbSJ9

Signature

MLzdiWUCEbInTH5YKRpqMmtQ4ptxeMM9LRIjEa8OUCY

@AramT87

JWT Claims

Claims represent the data contained within JWT as the payload.

These are defined as a dictionary of key,value pairs, where the key can be either predefined or custom, and the value can be any JSON value

There is a long list of predefined claims, but some of them are commonly used

JWT Claims

Most common Predefined (Registered) Claims are:

iss: Issuer
sub: Subject
aud: Audience
exp: Expiry time (in epoch)
nbf: Not before time
iat: Issued at time (in epoch)
jti: JWT unique Identifier

@AramT87

Decoding JWT

Since each part of a JWT is a base64 url-encoded string, then you can easily decode it.

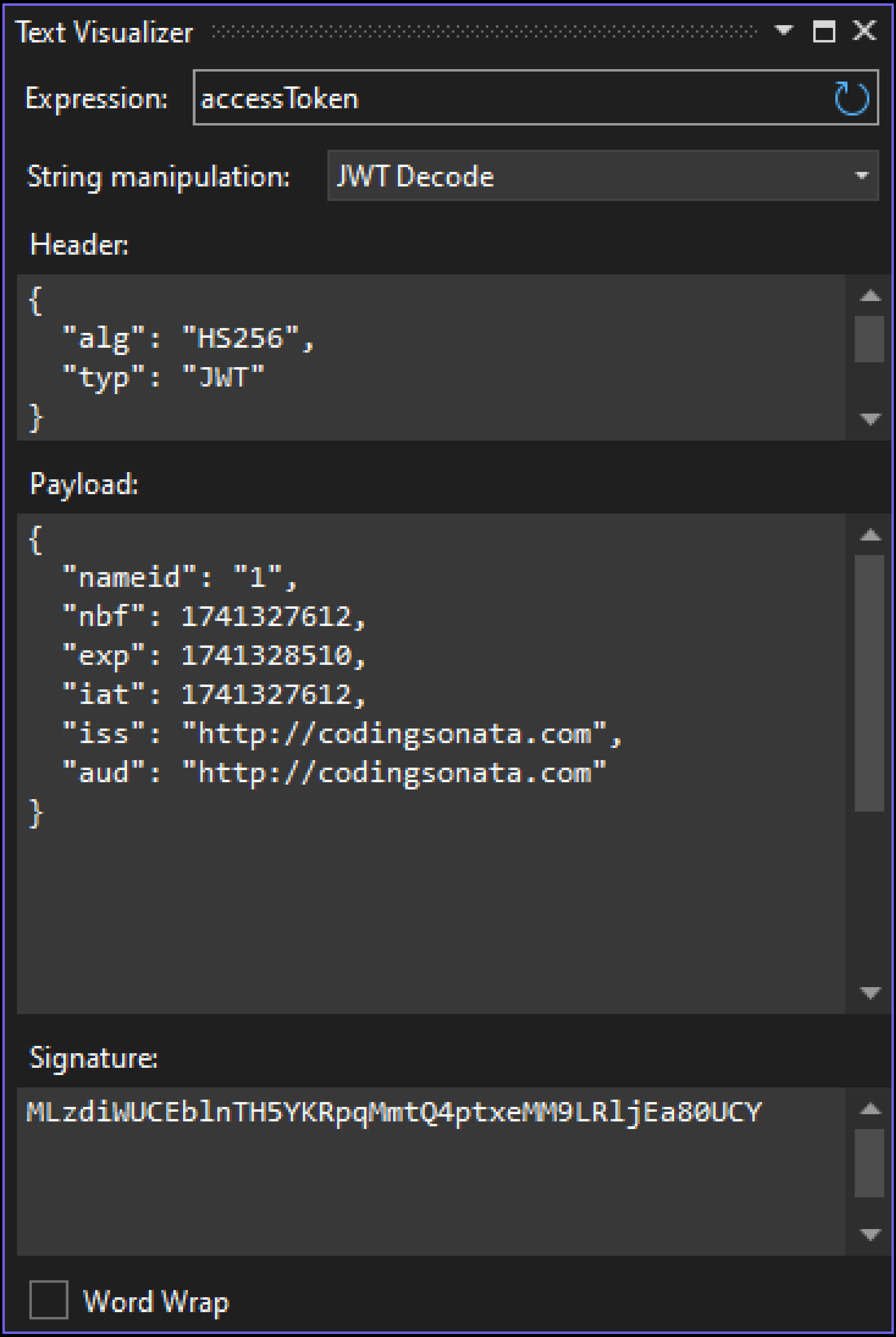
VS 2022 has a built-in support to decode any JWT while debugging

You can also use JWT.io to decode your JWT.

JWT.io also checks the signature if you put the secret used to sign the JWT

@AramT87

Decoding JWT in VS 2022



Expression: accessToken

String manipulation: JWT Decode

Header:

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

Payload:

```
{
  "nameid": "1",
  "nbf": 1741327612,
  "exp": 1741328510,
  "iat": 1741327612,
  "iss": "http://codingsonata.com",
  "aud": "http://codingsonata.com"
}
```

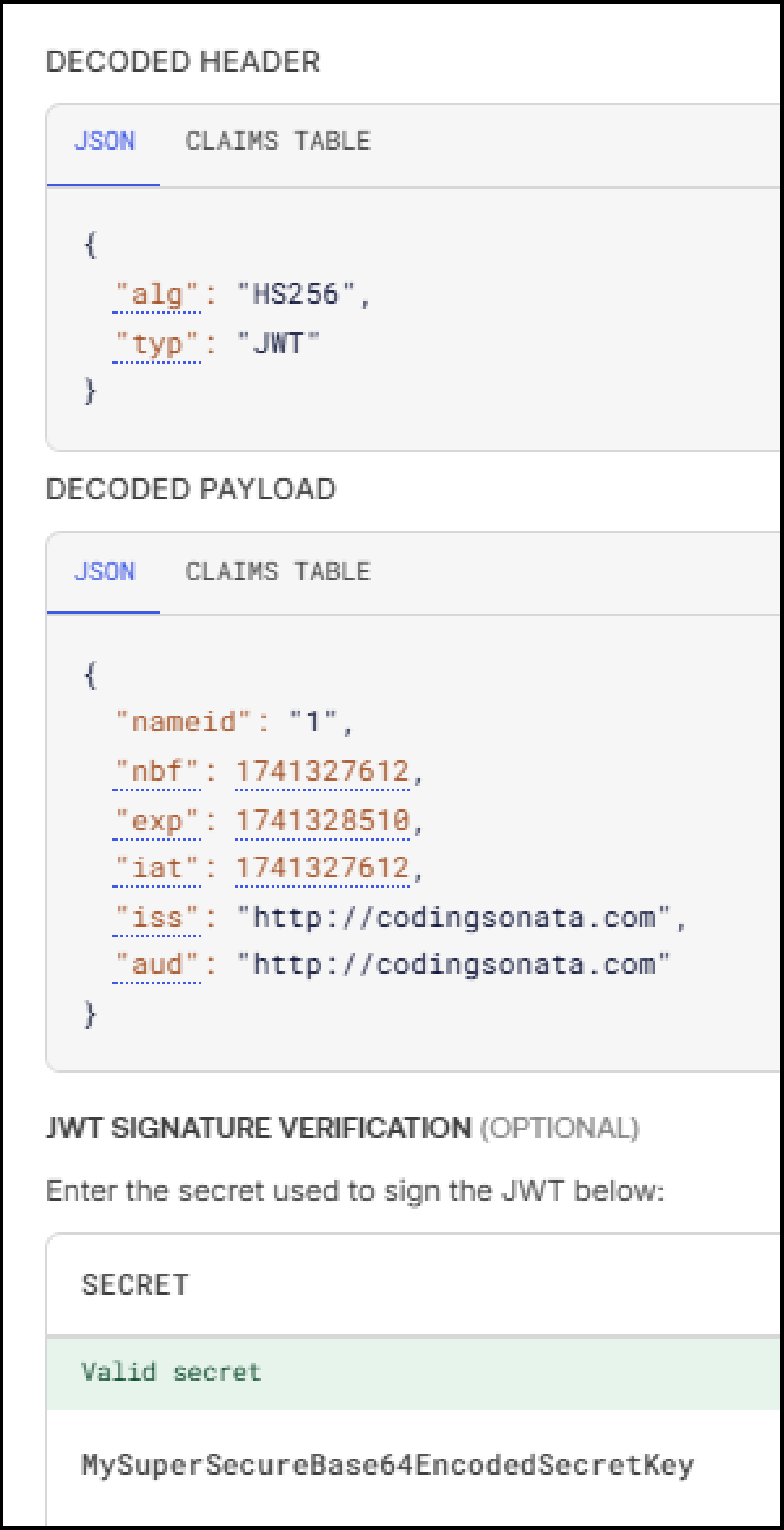
Signature:

```
MLzdiWUCEblnTH5YKRpqMmtQ4ptxeMM9LRljEa80UCY
```

□ Word Wrap

@AramT87

Decoding JWT in JWT.io



DECODED HEADER

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

DECODED PAYLOAD

```
{
  "nameid": "1",
  "nbf": 1741327612,
  "exp": 1741328510,
  "iat": 1741327612,
  "iss": "http://codingsonata.com",
  "aud": "http://codingsonata.com"
}
```

JWT SIGNATURE VERIFICATION (OPTIONAL)

Enter the secret used to sign the JWT below:

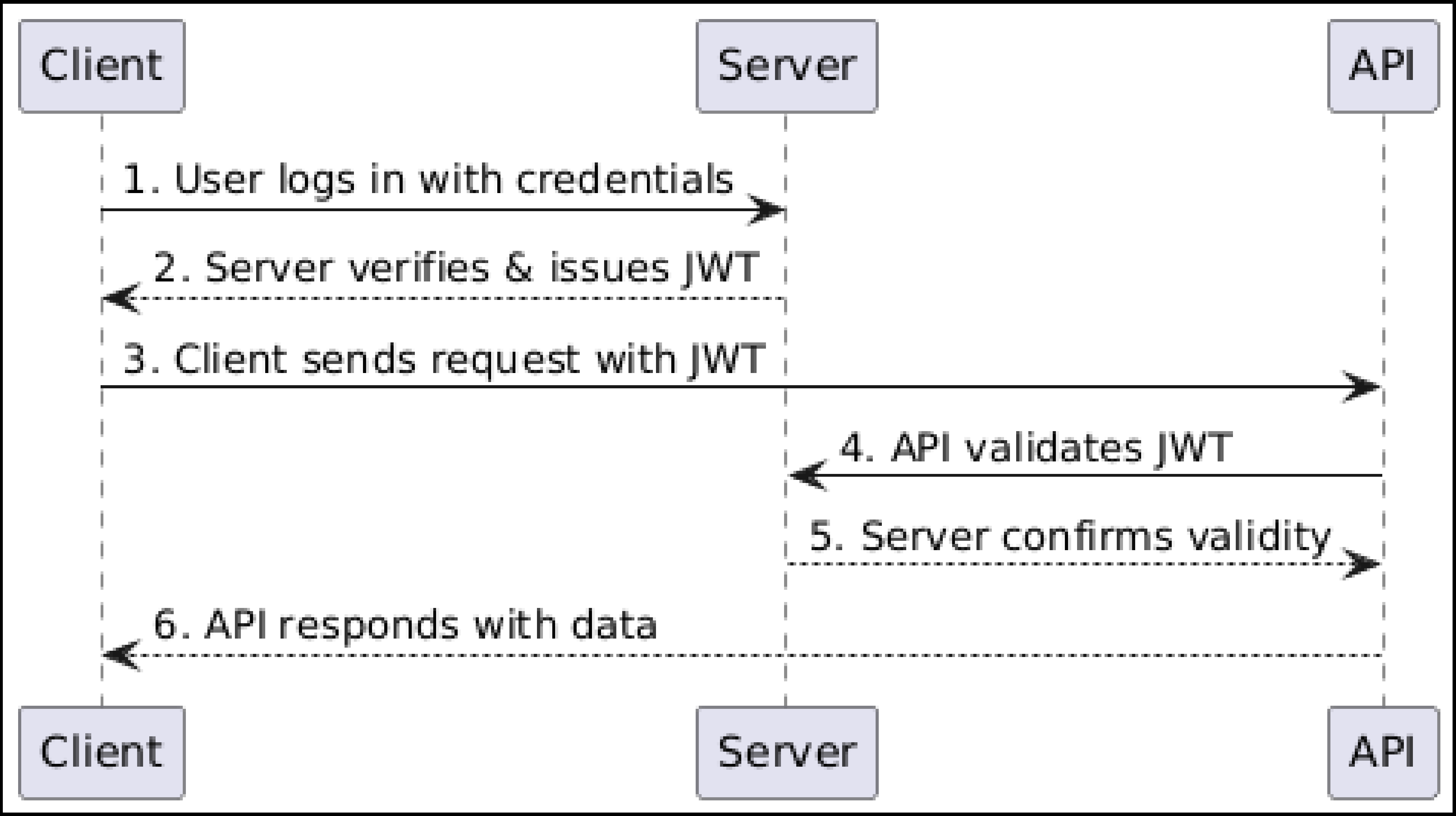
SECRET

Valid secret

MySuperSecureBase64EncodedSecretKey

@AramT87

Authentication with JWT



Client
Server
API
1. User logs in with credentials
2. Server verifies & issues JWT
3. Client sends request with JWT
4. API validates JWT
5. Server confirms validity
6. API responds with data
Client
Server
API

@AramT87

JWT Best Practices

Store the secret key in a secure place (environment variable or a vault), don’t keep it in code or in source control

Always use HTTPS to prevent man-in-the-middle attacks (interception).

Do not store sensitive data in JWTs unless you encrypt them

Set short expiry (exp), usually in few minutes time, and use refresh tokens for long sessions.

JWT Best Practices

On frontend, store JWTs in HTTP-only cookies, not localStorage.

Use SameSite=strict for cookies to prevent CSRF.

Avoid using the none algorithm type for signing the JWT, unless you are totally sure the JWT is already verified

Validate essential claims like:

- exp
- iss
- aud
- iat

@AramT87

Thank You

Follow me for more content

Aram Tchekrekjian

Microsoft® MVP Most Valuable Professional

AramT87

Get Free Tips and Tutorials in .NET and C#

Join 800+ Readers

CodingSonata.com/newsletters

<CodingSonata />