



JWT

JSON Web Tokens



!=




jwt.io by  Auth0

Discover by 

Konjugation "to take"


Infinitive

 to take

Simple past

 took

Past participle

 taken

JSON Web Tokens are
an open, industry standard **RFC 7519** method
for representing claims
securely between two parties.

What's a Token

EyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MzIyMDIyLCJpc3F1b3R5IjoiZm9udC51b3R5In0.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

→ ~~gibberish~~ **base64**

Base64 is an encoding scheme
that represents binary data
as an **ASCII string**.

→ A-Z a-z 0-9 + / =

→ 3 bytes = 4 chars

→ pads with „=“

UG9seWZvbiB6d2l0c2NoZXJuZCBhw59lbiBNw6R4Y2hlbnMgV
sO2Z2VsIFLDvGJlbiwgSm9naHVydCB1bmQgUXVhcms=

What's a Token

EyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWwiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c

- ~~gibberish~~ **base64**
- **header**.payload.signature
- Authorization
- Signed

What's a Token

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

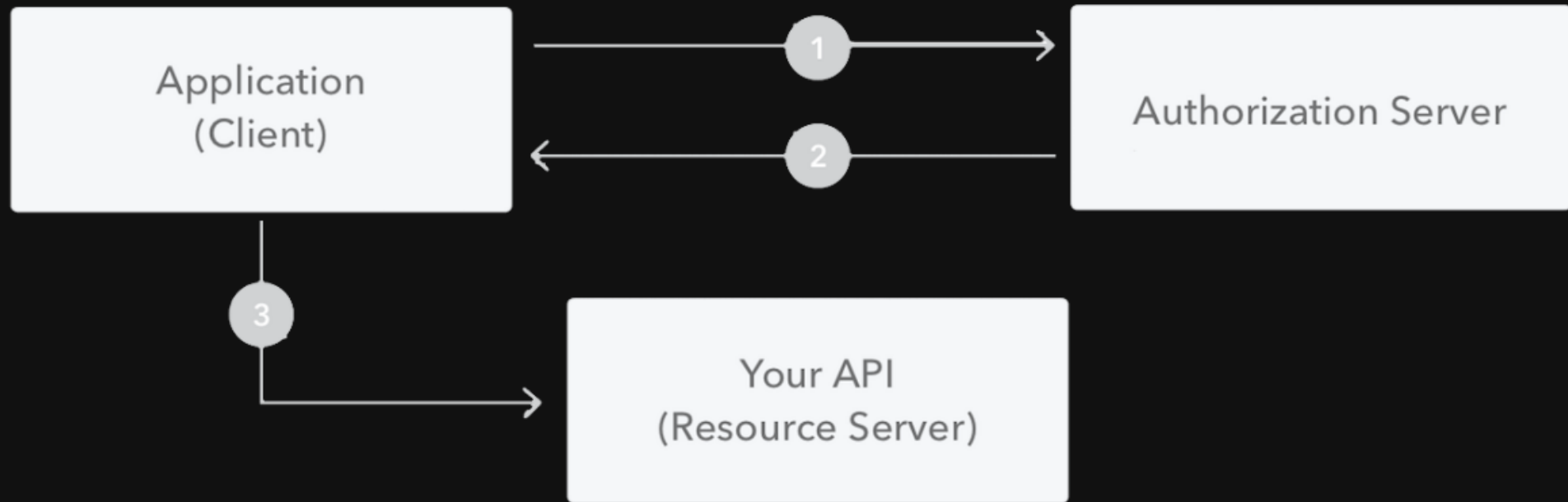
```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

```

HMACSHA256(
    base64UrlEncode(header) + "." +
    base64UrlEncode(payload),
    "your-256-bit-secret"
)

```

What's a Token



Why this Token

- JSON is readable
- JSON is well-known
- Can be signed asymmetrically

Be Careful

1. The „none“ algorithm

2. The algorithm

```
verify(string token, string verificationKey)
```

Thanks for listening!