AMSTERDAM 16 - 17 MAY 2017

{codemotion}

{ JWT, WTF?

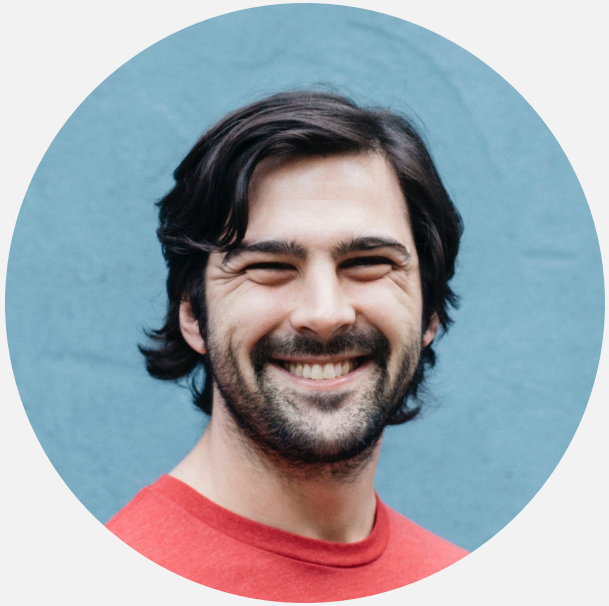
Phil Nash

Phil Nash

@philnash

http://philna.sh

philnash@twilio.com



twilio

ARE YOU READY FOR SOME ABBREVIATIONS?

JWT

JSON WEB TOKEN

RFC 7519

"JOT"

THERE'S MORE

JWS

JWE

JWK

JWA

RFCS

7515

7516

7517

7518

JOSE

RFC 7520

AAARGH

ACTUALLY

EMOJIS!

LET'S START AGAIN

JWT, WTF?

JWTs

- What are they?
- What can you use them for?
- How do they work?
- Pitfalls

WHAT'S A JWT?

JWT

"JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties."

JWT

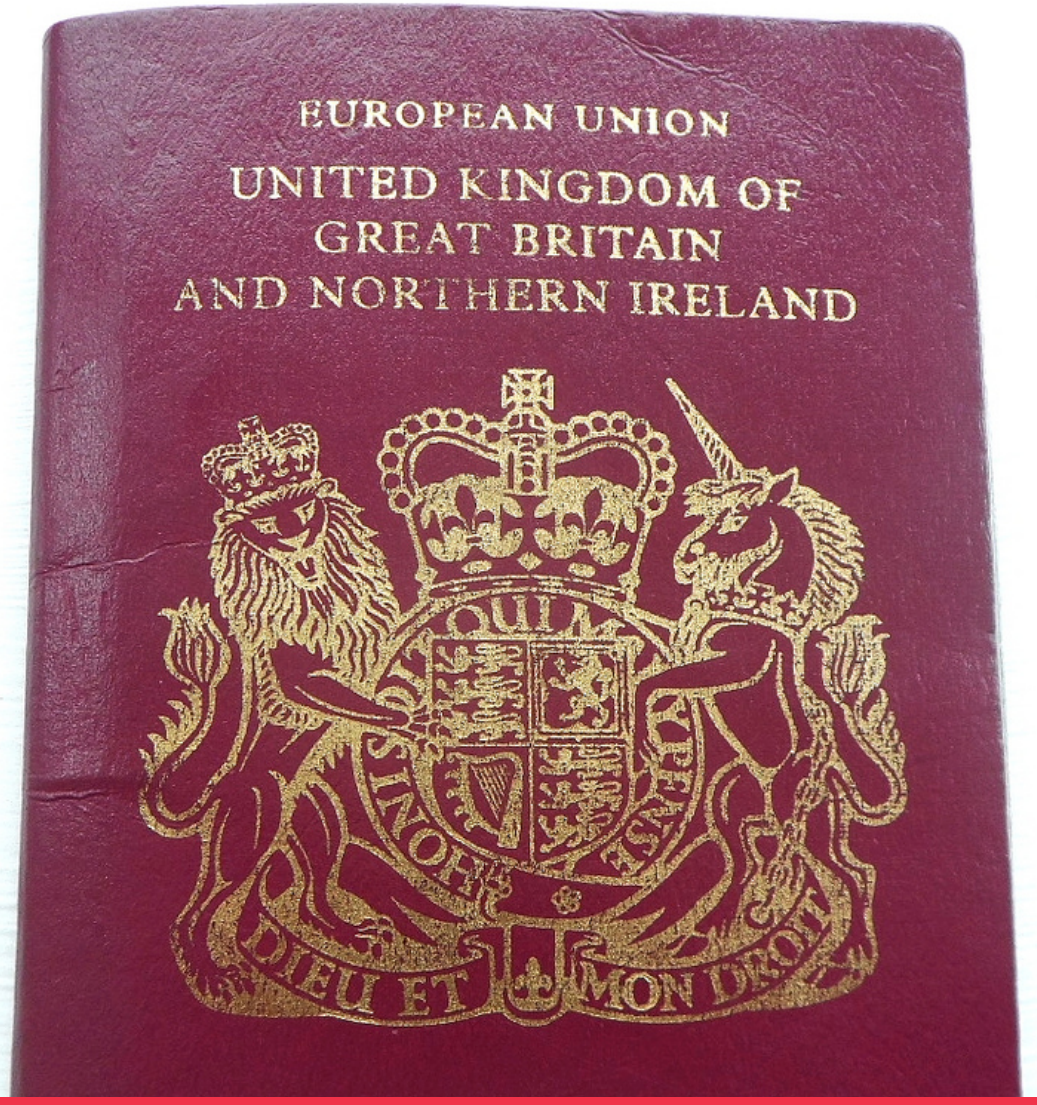
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiJwaGlsbmFzaEB0d2lsaW8uY29tIn0.
l9vi8Dt8Pds3QTBqNMnQGU0wDDWDv46RFIcqeOIPqDk

JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiJwaGlsbmFzaEB0d2lsaW8uY29tIn0.
l9vi8Dt8Pds3QTBqNMnQGU0wDDWDv46RFIcqeOIPqDk

JWT

```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "sub": "philnash@twilio.com"
}
```


EUROPEAN UNION
UNITED KINGDOM OF
GREAT BRITAIN
AND NORTHERN IRELAND
DIEU ET MON DROIT

WHAT CAN YOU USE THEM FOR?

STATELESS SESSIONS

MICROSERVICE ARCHITECTURE

OPENID CONNECT

CLIENT SIDE AUTH FOR 3RD PARTY SERVICES

HOW DO THEY WORK?

CREATING A JWT

Creating a JWT

```
const header = {
  "alg": "HS256",
  "typ": "JWT"
}
const payload = {
  "sub": "philnash@twilio.com"
}
```

CLAIMS

Header Claims

```
"typ": "JWT"
```

Header Claims - Unsecured

```
"alg": "none"
```

Header Claims - Secured

```
"alg": "HS256"
```

Payload Claims

- `"iss"` - issuer
- `"sub"` - subject
- `"aud"` - audience
- `"exp"` - expires at
- `"nbf"` - not before
- `"iat"` - issued at
- `"jti"` - JWT ID

Payload Claims

Anything you want!

Creating a JWT

```
const header = {
  "alg": "HS256",
  "typ": "JWT"
}
const payload = {
  "sub": "philnash@twilio.com"
}
```

ENCODE THE HEADER AND PAYLOAD

Base64url

```
encodedHeader = new Buffer(JSON.stringify(header))
  .toString('base64')
  .replace(/=/g, "")
  .replace(/\+/g, "-")
  .replace(/\//g, "_");
```

Base64url

```
encodedPayload = new Buffer(JSON.stringify(payload))
  .toString('base64')
  .replace(/=/g, "")
  .replace(/\+/g, "-")
  .replace(/\//g, "_");
```

SIGN THE ENCODED

HEADER AND PAYLOAD

HMAC SHA256

```
const crypto = require('crypto');

const hmac = crypto.createHmac('sha256', 'secret');
hmac.update(`${encodedHeader}.${encodedPayload}`);
const signature = hmac.digest('base64');
```

The finished JWT

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
eyJzdWIiOiJwaGlsbmFzaEB0d2lsaW8uY29tIn0.
l9vi8Dt8Pds3QTBqNMnQGU0wDDWDv46RFIcqeOIPqDk
```

VERIFYING A JWT

Verifying a JWT

```
[
  encodedHeader,
  encodedPayload,
  signature
] = jwt.split('.');
```

Decode the header

```
const decodedHeader = JSON.parse(
  new Buffer(encodedHeader, 'base64').toString('ascii')
)
```

Decode the payload

```
const decodedPayload = JSON.parse(
  new Buffer(encodedPayload, 'base64').toString('ascii')
)
```

HMAC SHA256

```
const crypto = require('crypto');

const hmac = crypto.createHmac('sha256', 'secret');
hmac.update(`${encodedHeader}.${encodedPayload}`);
const generatedSignature = hmac.digest('base64');
```

Compare

```
secureCompare(signature, generatedSignature);
```

JWT Playground

https://jwt.io

PITFALLS

DATA IS PUBLIC

SIGNING ALGORITHM

JWT

```
{
  "alg": "HS256",
  "typ": "JWT"
}
{
  "sub": "philnash@twilio.com"
}
```

JWT

```
{
  "alg": "none",
  "typ": "JWT"
}
{
  "sub": "philnash@twilio.com"
}
```

ALWAYS VERIFY WITH AN

EXPECTED ALGORITHM

PUBLIC KEYS AND ENCRYPTION

WHAT CAN YOU USE THEM FOR?

STATELESS SESSIONS

Stateless sessions - revocation

- `exp` claim - token expiry time
- Without state, you can't revoke individual tokens except by expiry
- Requires a blacklist of revoked tokens to check against

Stateless sessions - storage

- Cookies
  - ensure you have CSRF protection
- localStorage
  - vulnerable to XSS
  - requires JS to store and insert as an Authentication header

MICROSERVICE ARCHITECTURE

Microservice architecture

- Authentication server signs tokens with private key
- Other servers can verify with public key

OPENID CONNECT

CLIENT SIDE AUTH FOR 3RD PARTY SERVICES

JWT, WTF?

JWT, WTF?

- https://jwt.io
- RFC 7519
- JWTs VS Sessions
- Stop using JWT for sessions
- Use JWT the Right Way

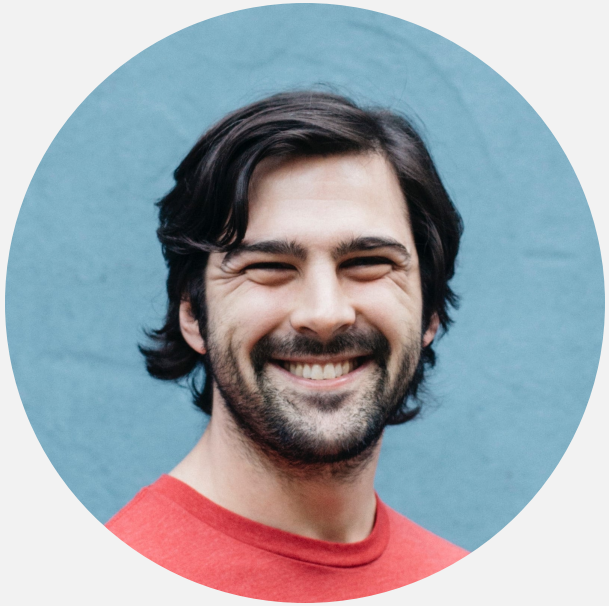
THANKS!

Thanks!

@philnash

http://philna.sh

philnash@twilio.com



twilio