Json Web Token

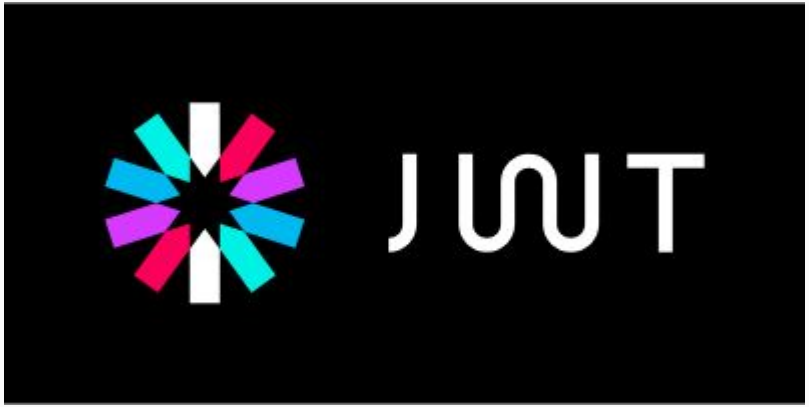
Yuthana + Rossukhon

Growth Session #19 - October 11-12 2018

Objectives

- Check how does the JWT works
- Check the Hadex authentication flow

What is the JWT?



The standard way to securely transmit the data between parties as a JSON object

JWT Structure

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.-rUA6p_U6nMrGI76SSOvS376iebCGDwtN5hxKjHFCFk

JWT Structure - Header

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM
0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE
6SSOvS376iebCGDwtN5

1. Header - Define the type (Which is JWT) and the signing algorithm

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

JWT Structure - Payload

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM
0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2
MjM5MDIyfQ.-rUA6p
KjHFCFk

2. Payload - The data to transfer

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

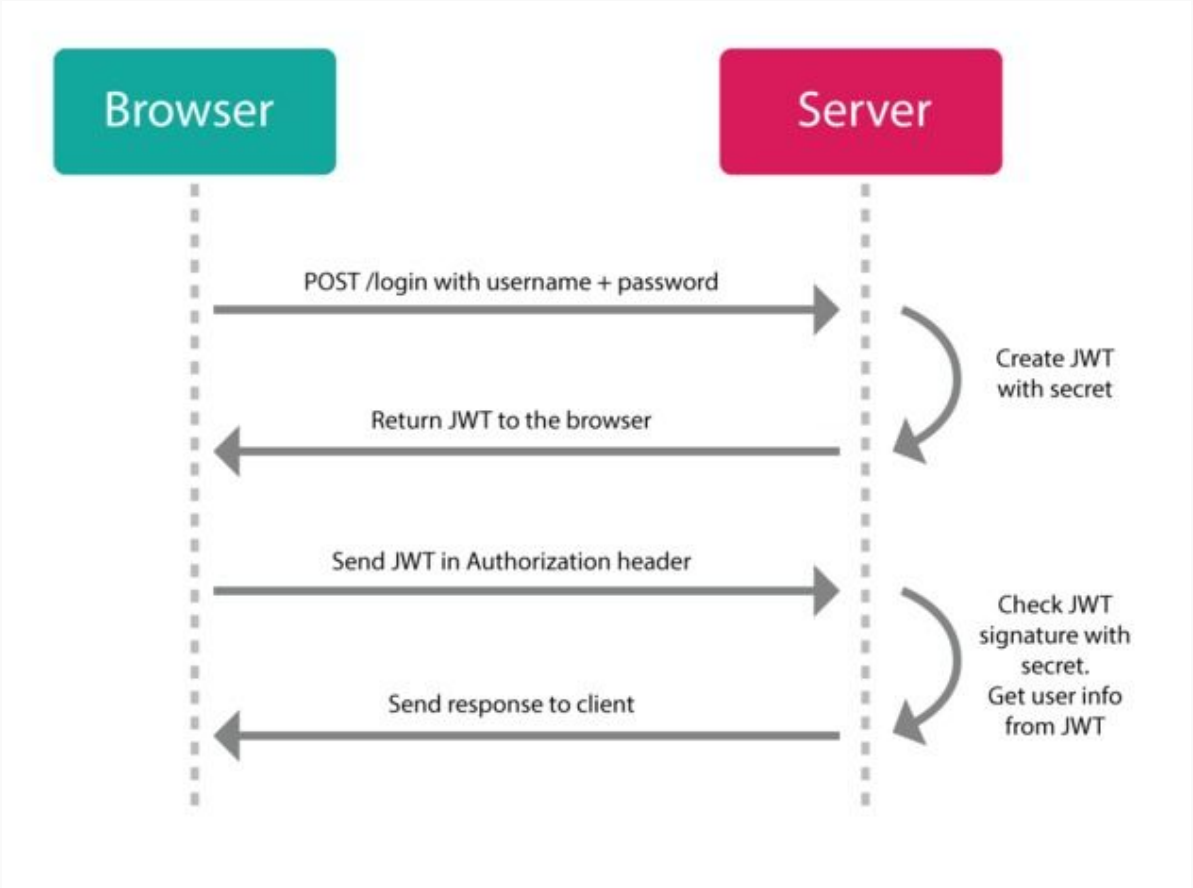
JWT Structure - Signature

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM
0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2
MjM5MDIyfQ.-rUA6p_U6nMrGI76SSOvS376iebCGDwtN5hx
KjHFCFk

3. Signature - Take all parts together and sign with the algorithm specified in the header

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  MySecretKey
)
```

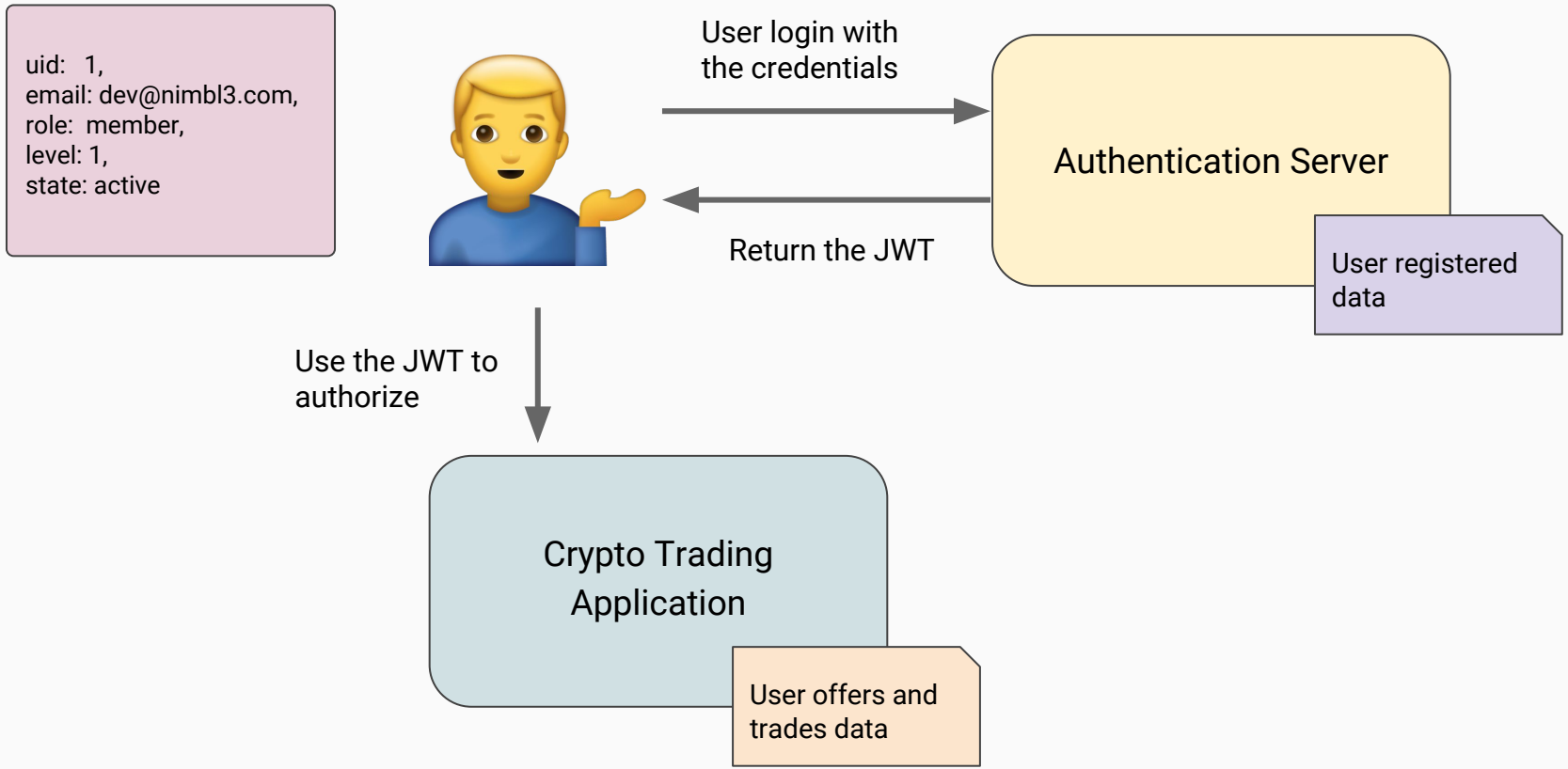
Authentication Flow



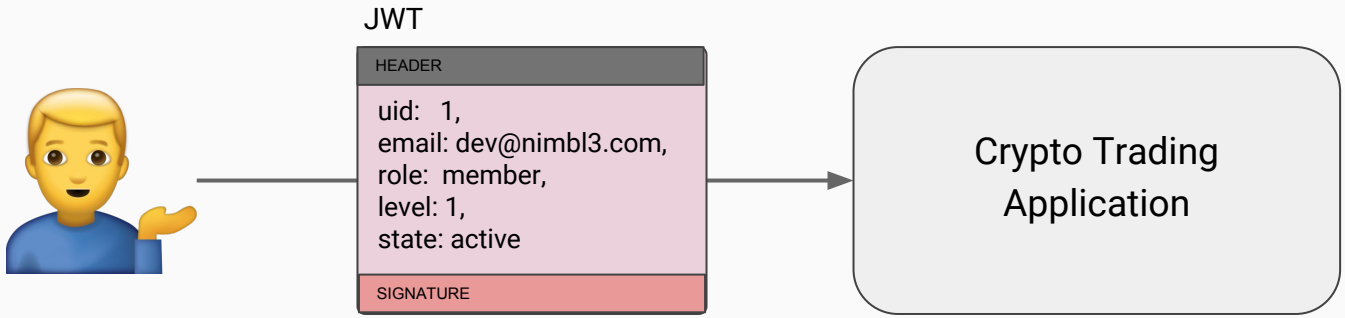
Benefits of Token-based Authentication

- **Cross-domain**: A token-based approach allows you to make AJAX calls to any server, on any domain, because you use an HTTP header to transmit the user information.
- **Stateless:** Tokens are stateless. There is no need to keep a session store since the token is a self-contained entity that stores all the user information in it.
- **Mobile Ready:** Cookies are a problem when it comes to storing user information in native mobile applications. Adopting a token-based approach simplifies this saving process significantly.
- **Performance:** In terms of server-side load, a network roundtrip is likely to take more time than calculating an HMACSHA256 code to validate a token and parsing its contents. This makes token-based authentication faster than the traditional alternative.

Case Study - Hadex



Case study - Hadex



Public key

vFoGU5I41hMZaKKem+KwKltjOTjoLkQ9er9nqAJa03aQDsxWVyE7bQMTm1Tf7t4GvqbWX
Ck2bVB9EKyMD9j/JgEupUz44lonFHGtNHxz8rEgfc45HpfpNGfVlUei7eJj6CTpESSFF7H30
z/bC4REDwjbyE226wldjTxMk1YDx3C4pr/ugQztQSxhEvelpAaiZh/PVdaXop6IWTJrJCMZ/f
f/JVvRNUG6zGwWjONwpBbx1ehJlF1YKgF2iszkwUrXVobacf1NKAh1aKkh8emuoCa2Azfr
Ni1xfRH2kDXIIKWQPMTwT3A6GrUYXYPXz4bUJDe3hnqnt6fj7o8rCMc2WQ==

Hadex - How To Set It Up

Authentication App

- doorkeeper
- doorkeeper-jwt

Crypto Trading App

- jwt

Hadex - Problems

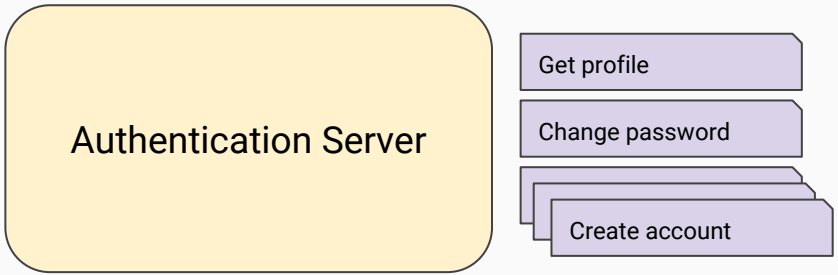
1. How to display or update the user profile data in the Trading app?

2. After user updated his/her profile on the authentication app, how the data in the Trading app will get updated?

Hadex - Problems

1. How to display the user profile data in the Trading app?

⇒ Access the user data through the auth app provided api using user token



Hadex - Problems

2. After user updated the profile on the authentication app, How the data in the Trading app will get updated? - Password changed, Role/Verified level changed

- Invalidate the token and the user re-login to the Trading app again?
- Use short-lived token?
- Periodically sync user profile?

Thanks!

Contact Nimbl3

hello@nimbl3.com

399 Sukhumvit Road, Interchange 21
Klongtoey nua, Wattana
Bangkok 10110

28C Stanley St,
Singapore 068737

20th Floor, Central Tower
28 Queen's Road
Central, Hong Kong

nimbl3.com