JWTs - What Ruby Developers need to know

Dan Moore

Chicago Ruby

Mar 2, 2021

@mooreds

FusionAuth

About FusionAuth

- Drop in user data store
- Multiple editions including community
- Supports
  - OAuth grants
  - SAML
  - Passwordless
  - And more
- Produce a whole lot of JWTs

About me

@mooreds

FusionAuth

About me

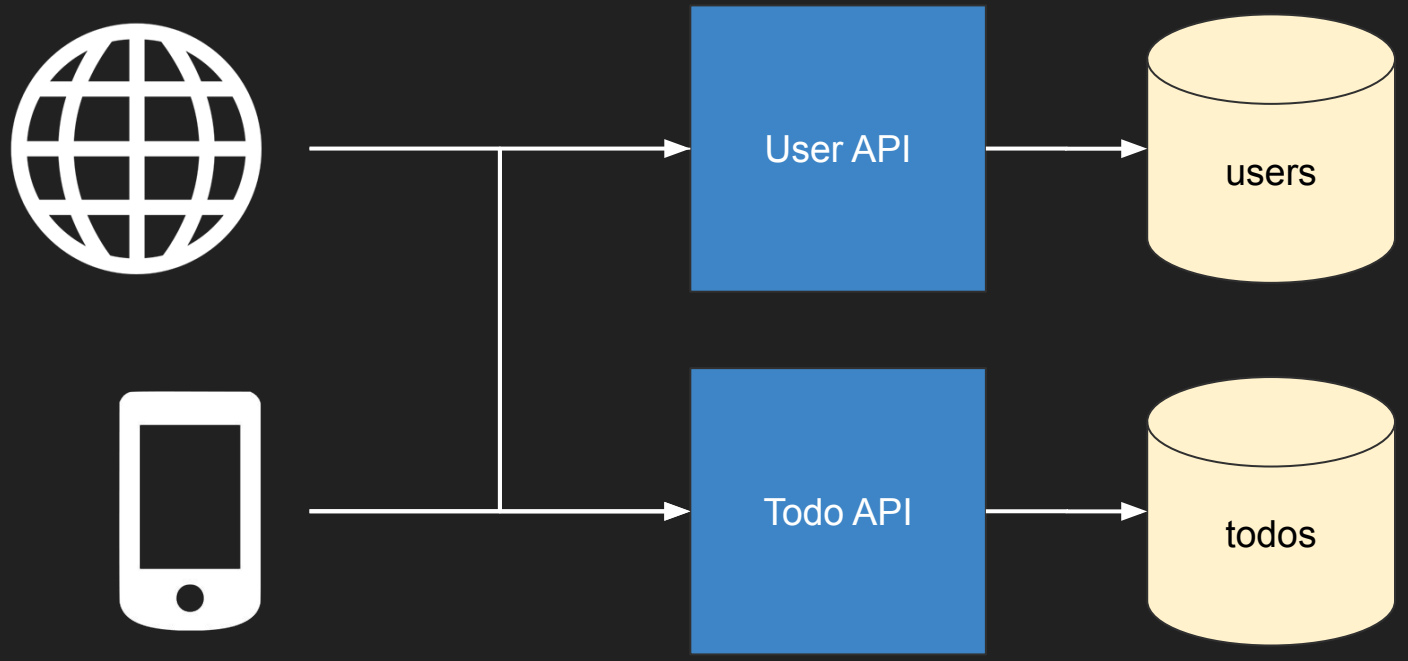
- Who cares

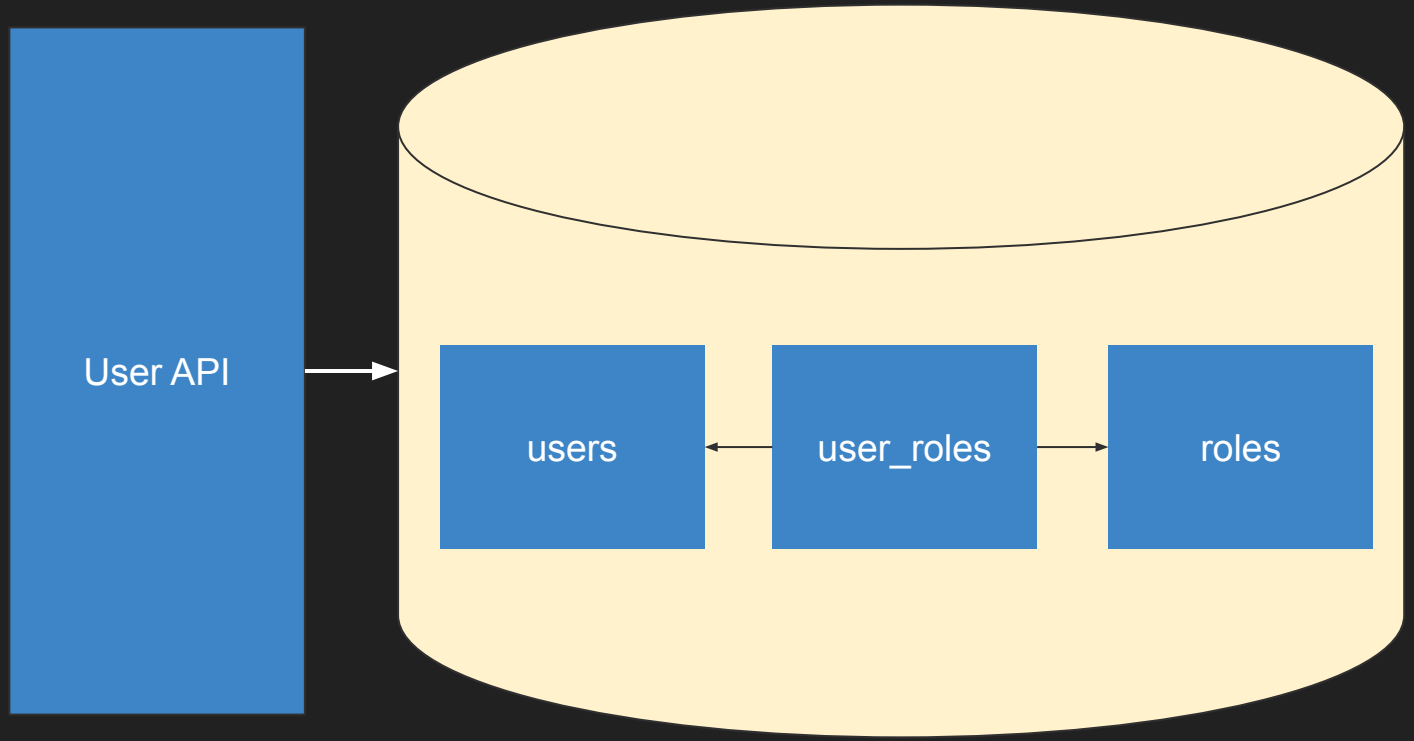
Questions

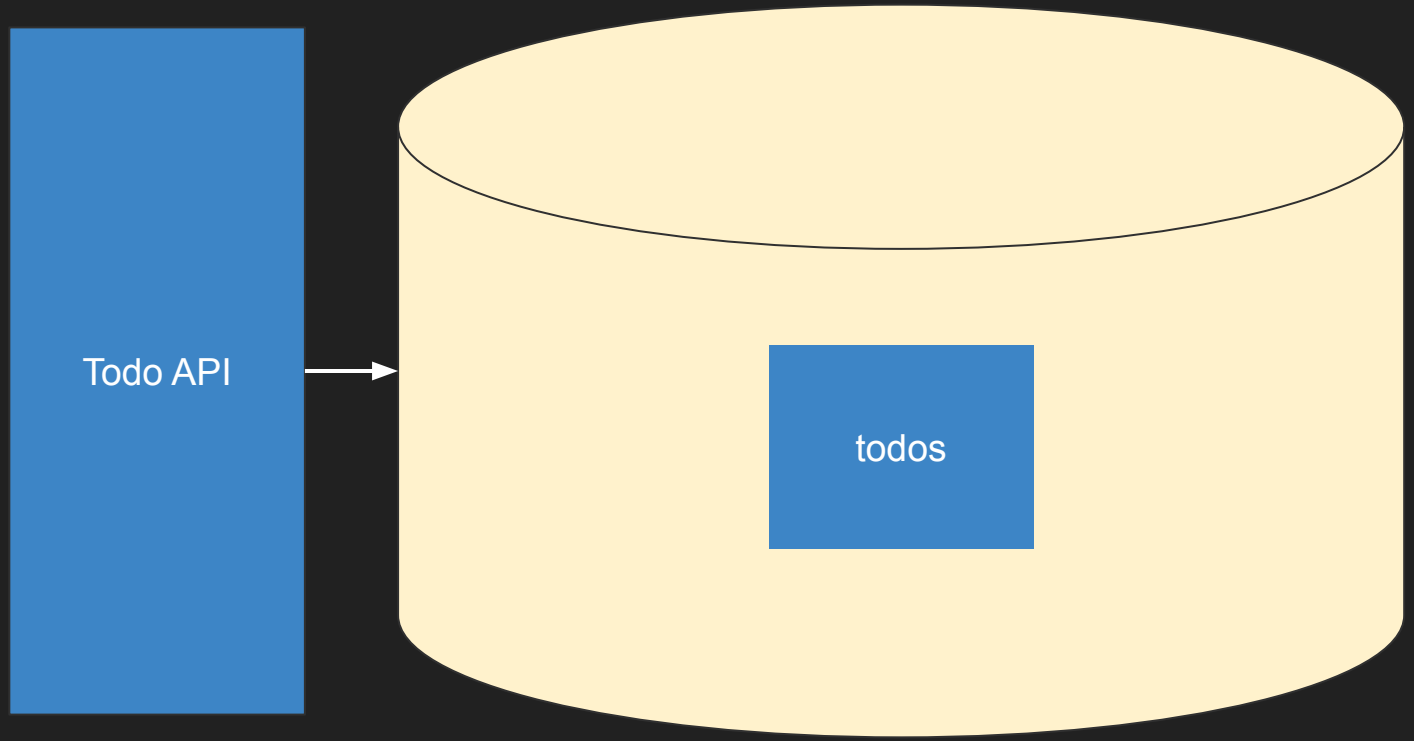
- In the chat or with your voice
- If I lag, please tell me
- Free t-shirt

JWTs - Briefly

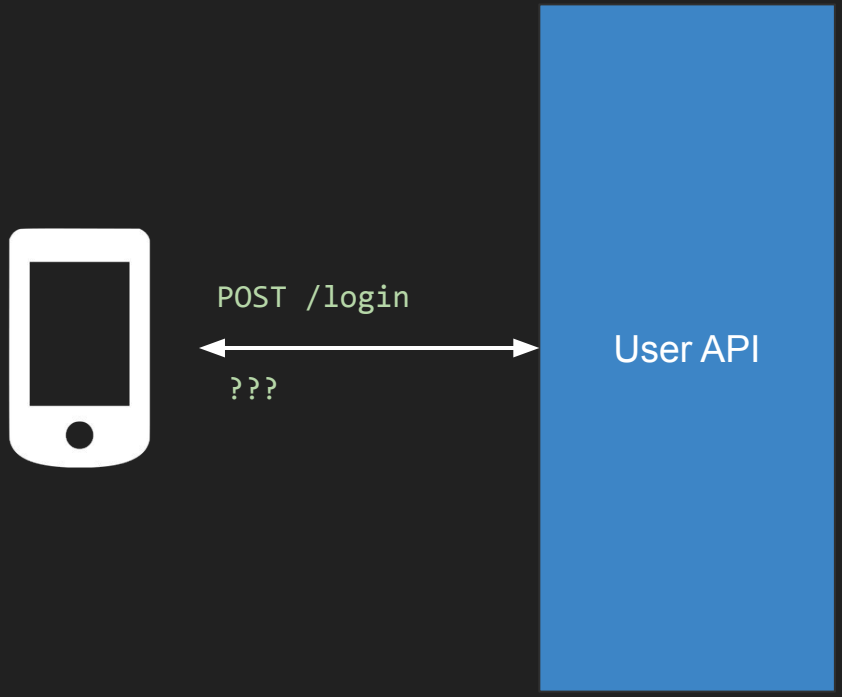
- JSON Web Token
- Pronounced ‘jot’
- Standard - RFC 7519
- Stateless, portable tokens of identity
- Great for APIs
- Produced by many IdP servers
- Bearer tokens

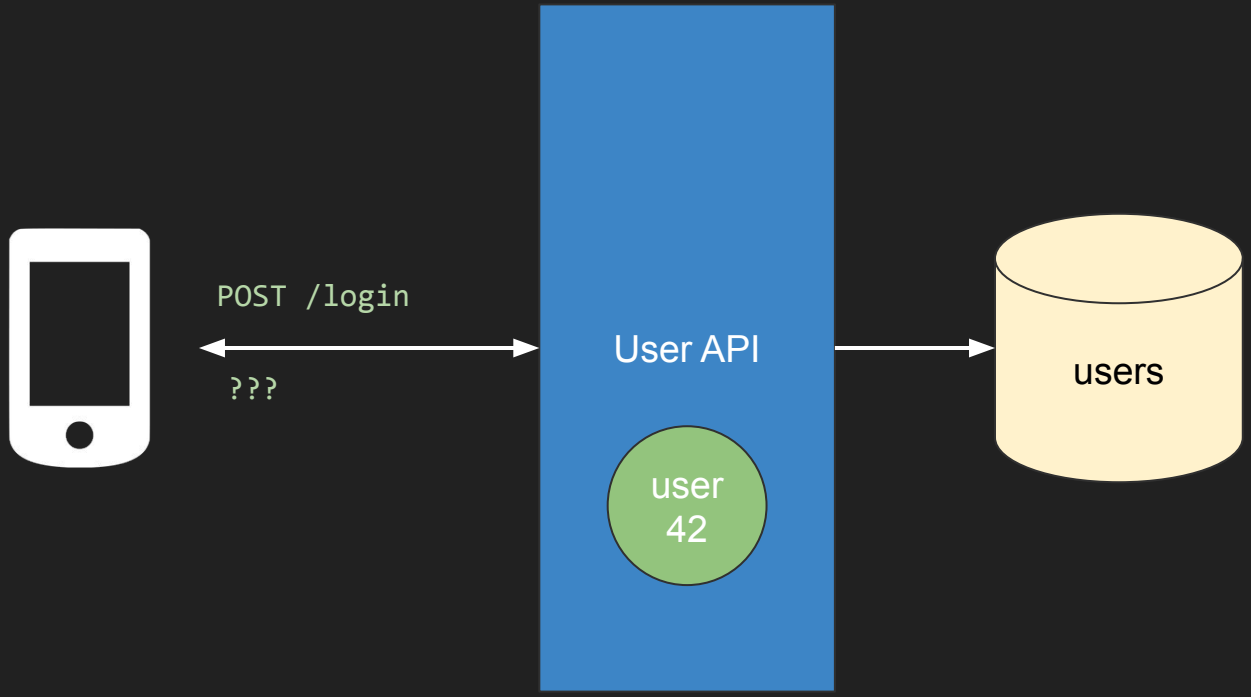

User API
users
Todo API
todos

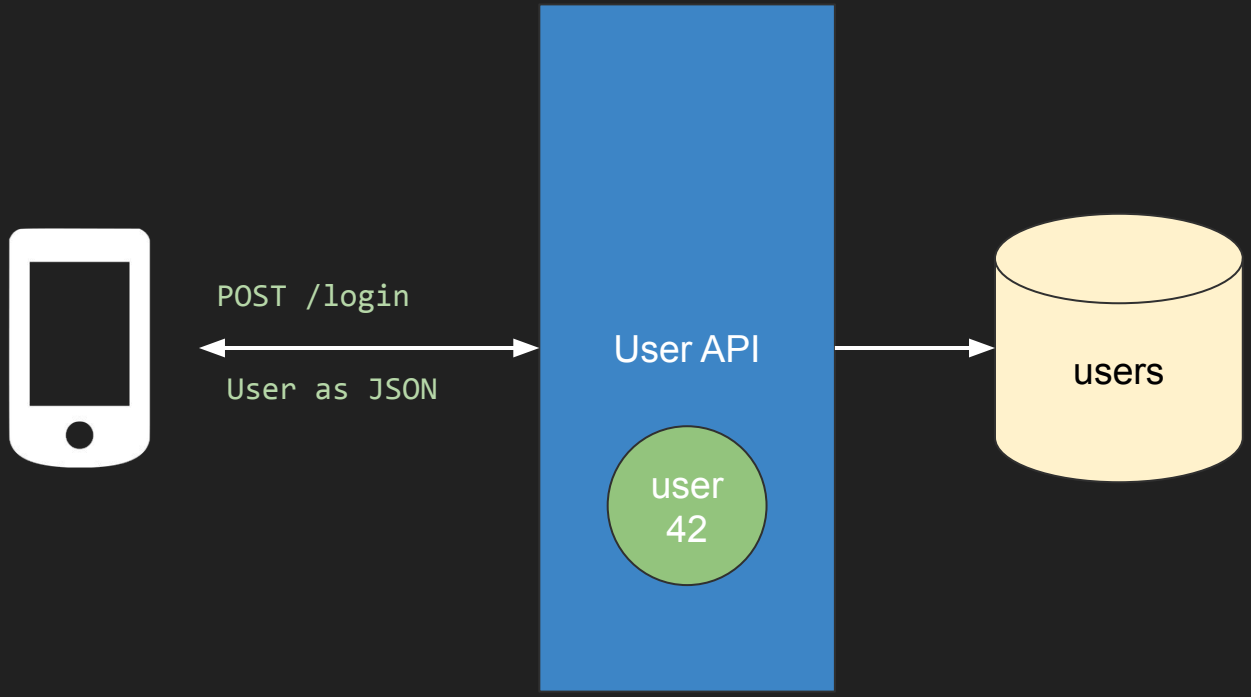

User API
users
user_roles
roles


Todo API
todos

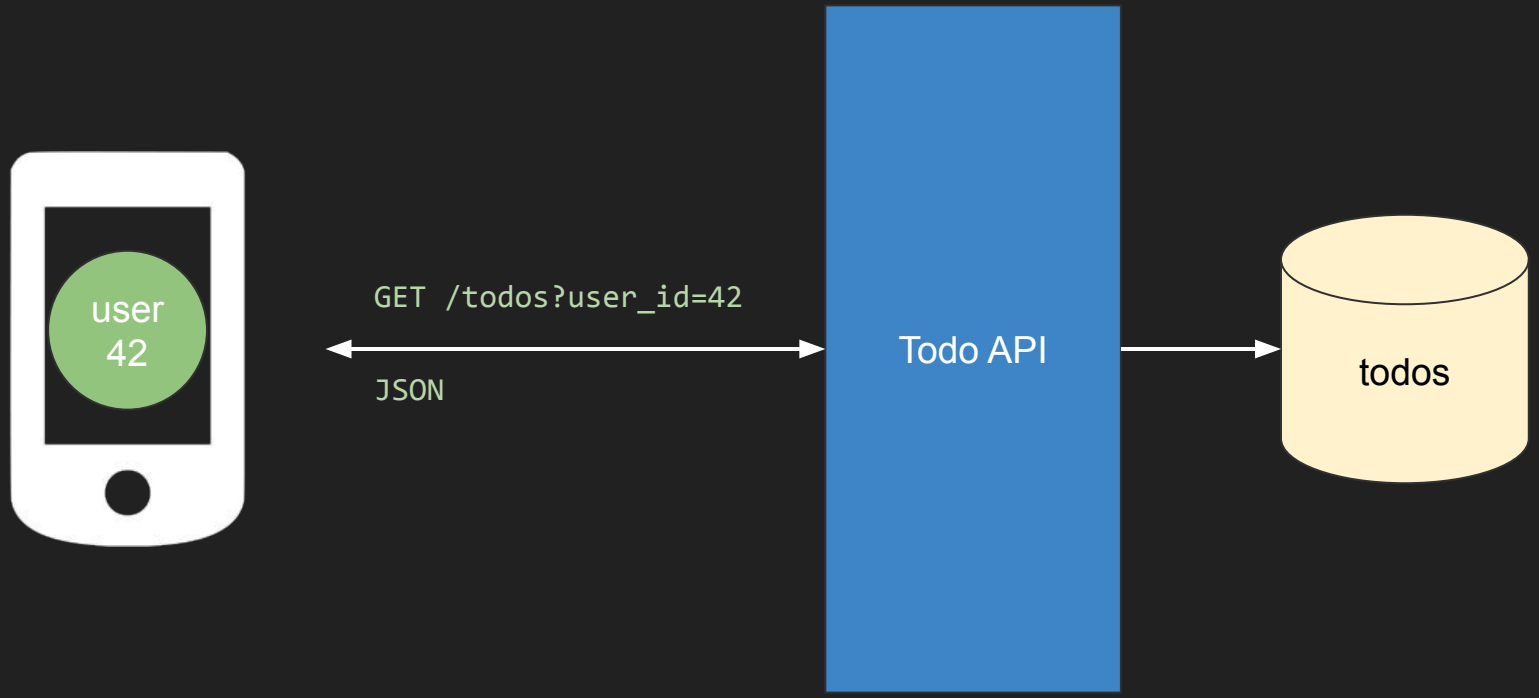
```
CREATE TABLE todos (
  id INT NOT NULL,
  text TEXT NOT NULL,
  user_id INT NOT NULL,
  PRIMARY KEY (id)
);
```


POST /login
???
User API

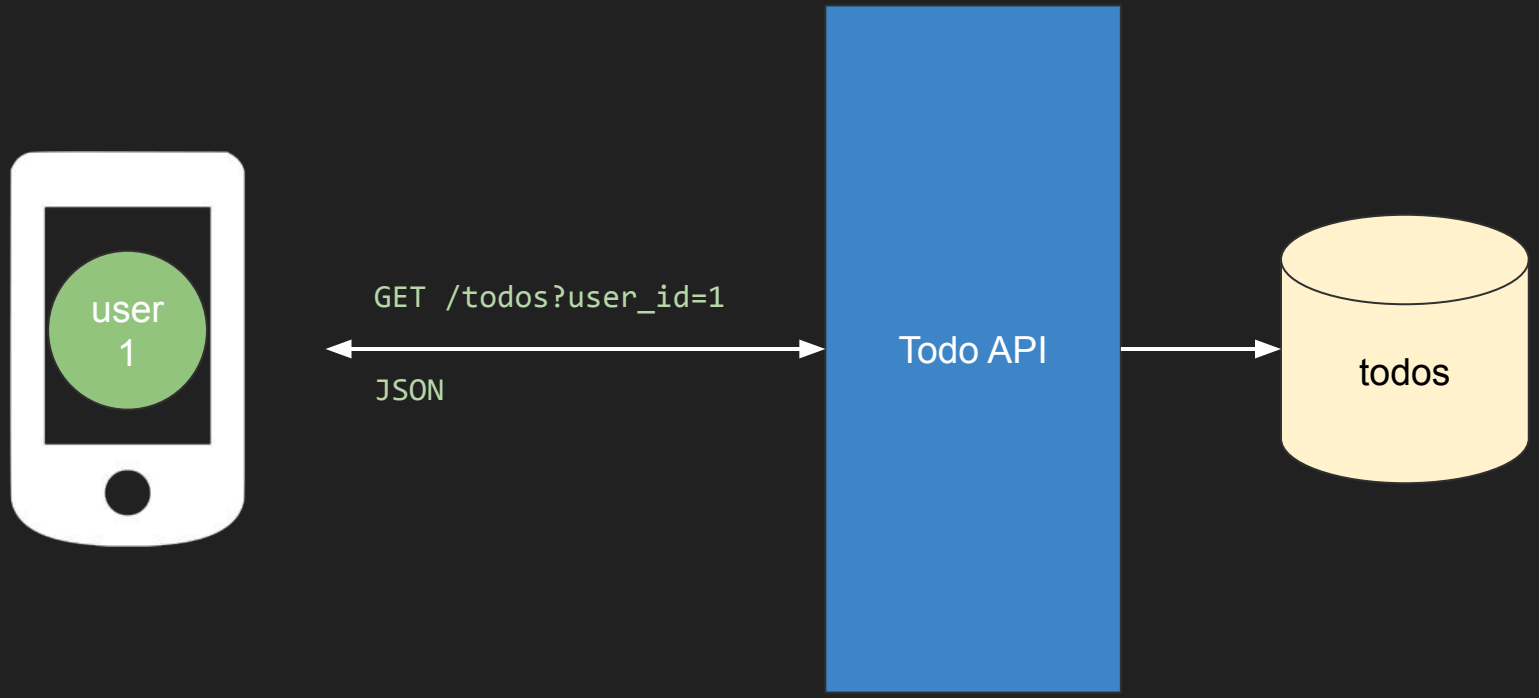

POST /login
???
User API
user
42
users


POST /login
User as JSON
User API
user
42
users

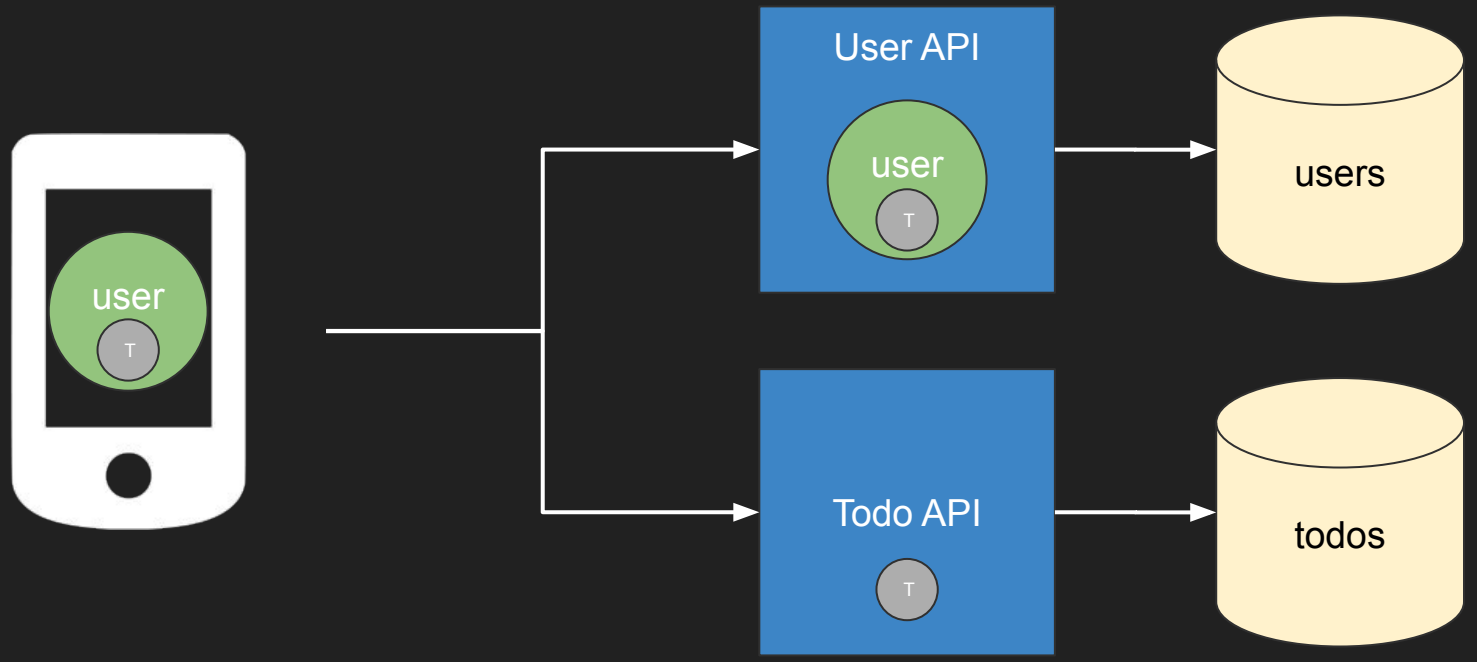
```
{
  "user": {
    "id": 42,
    "name": "Dan Moore",
    "email": "dan@fusionauth.io",
    "roles": ["admin"]
  }
}
```

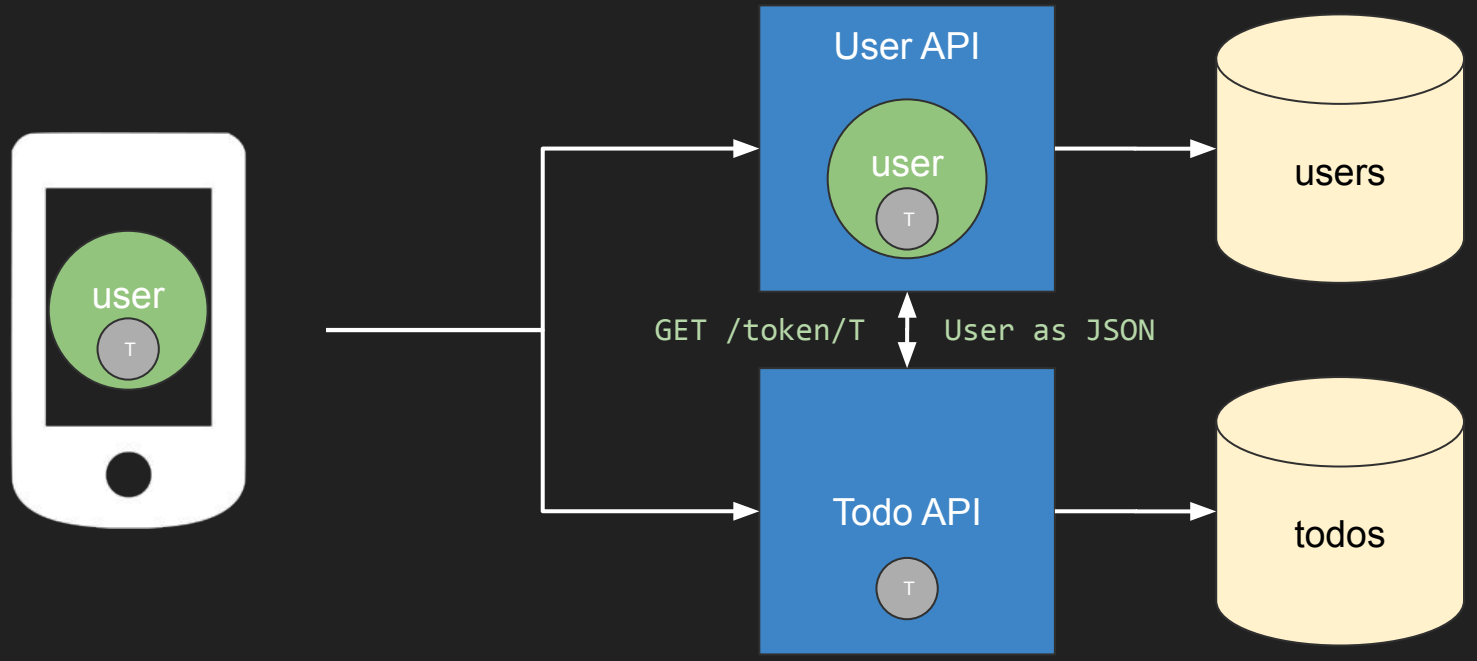

user
42
GET /todos?user_id=42
JSON
Todo API
todos

Danger Will Robinson!


user
1
GET /todos?user_id=1
JSON
Todo API
todos

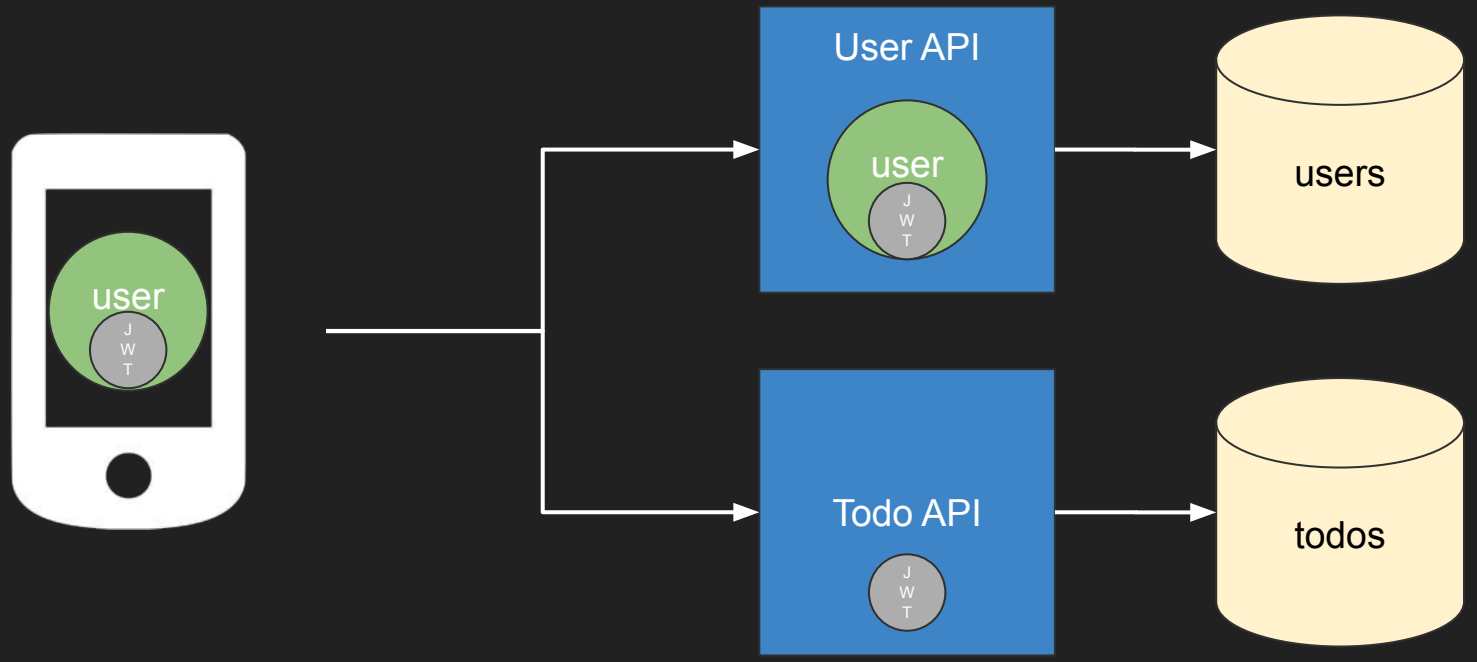
Get milk


user
T
User API
user
T
users
Todo API
T
todos


user
T
User API
user
T
users
GET /token/T
User as JSON
Todo API
T
todos

Tokens

- There must be a User -> Token mapping
- In memory or in database
- Makes the User API slightly stateful
- Can be very chatty
- Couples the User API to EVERYTHING (almost)


user
J
W
T
User API
user
J
W
T
users
Todo API
J
W
T
todos

JWT

- Can be validated by Todo API without calling User API
- Signed
  - Public/private key pair
  - Symmetric key
- Contains roles and other metadata

JWT

eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJmdXNpb25hdXRoLmlvIiwiZXhwIjoxNTg5MjI3MDA2LCJhdWQiOiIyMzhkNDc5My03MGRlLTQxODMtOTcwNy00OGVkOGVjZDE5ZDkiLCJzdWIiOiIxOTAxNmI3My0zZmZhLTRiMjYtODBkOC1hYTkyODc3MzgzNzciLCJuYW1lIjoiRGFuIE1vb3JlIiwicm9sZXMiOlsiUkVUUklFVkVfVE9ET1MiXX0.dlXJ3bdjsN9ivekeYMJdeA5jla6cKqxTkBixijRDpSTdDwwtSX4j0MdBsQhrYnJqVRdtBAufRC3T5hQpKVPgskP1nfkRqSJx1awZajeinab76HD_mdm5RwtuXycBgJ9KJt3JPAkyLSpeT-SrWO1h2gLt4pioP8GtSpIZocEXMcKkeOL7-8KyZAi1VYYQN3aiy0ZkbaKq7_nj2SrMYw4myRaAIYj0Ngamx9DlZrVfmSM4xn6ZwcvT17y_Ff0VX9T-Z6x9dEIPxhi8EVBDzyclmhaULn_9ALp2oIIIdACqzgoGZc2MwC0DED7-IIRt0Qi20H9nfyGavfDs80aGcubVLQ

@mooreds

FusionAuth

JWT Header

```
eyJhbGciOiJSUzI1NiJ9
```

=

```
{
  "alg": "HS256"
}
```

JWT Body

eyJpc3MiOiJmdXNpb25hdXRoLmlvIiwiZXhwIjoxNTg5MjI3MDA2LCJhdWQiOiIyMzhkNDc5My03MGRlLTQxODMtOTcwNy00OGVkOGVjZDE5ZDkiLCJzdWIiOiIxOTAxNmI3My0zZmZhLTRiMjYtODBkOC1hYTkyODc3Mzg2NzciLCJuYW1lIjoiRGFuIE1vb3JlIiwicm9sZXMiOlsiUkVUUklFVkVfVE9ET1MiXX0

=

```
{
  "iss": "fusionauth.io",
  "exp": 1589227006,
  "aud": "238d4793-70de-4183-9707-48ed8ecd19d9",
  "sub": "19016b73-3ffa-4b26-80d8-aa9287738677",
  "name": "Dan Moore",
  "roles": ["RETRIEVE_TODOS"]
}
```

JWT Signature

```
dlXJ3bdjsN9ivekeYMJdeA5jla6cKqxTkBixijRDpSTdDwwtSX4j0MdBsQhrYn
JqVRdtBAufRC3T5hQpKVPgskP1nfkRqSJx1awZajeinab76HD_mdm5RwtuXycB
gJ9KJt3JPAkyLSpeT-SrWO1h2gLt4pioP8GtSpIZocEXMcKkeOL7-8KyZAi1VY
YQN3aiy0ZkbaKq7_nj2SrMYw4myRaAIYj0Ngamx9DlZrVfmSM4xn6ZwcvT17y_
Ff0VX9T-Z6x9dEIPxhi8EVBDzyclmhaULn_9ALp2oIIIdACqzgoGZc2MwC0DED
7-IIRt0Qi20H9nfyGavfDs80aGcubVLQ
```

=

RSA/HMAC/Elliptical Signature

```
select * from todos where user_id =
‘19016b73-3ffa-4b26-80d8-aa9287738677’;
```

Questions?

@mooreds

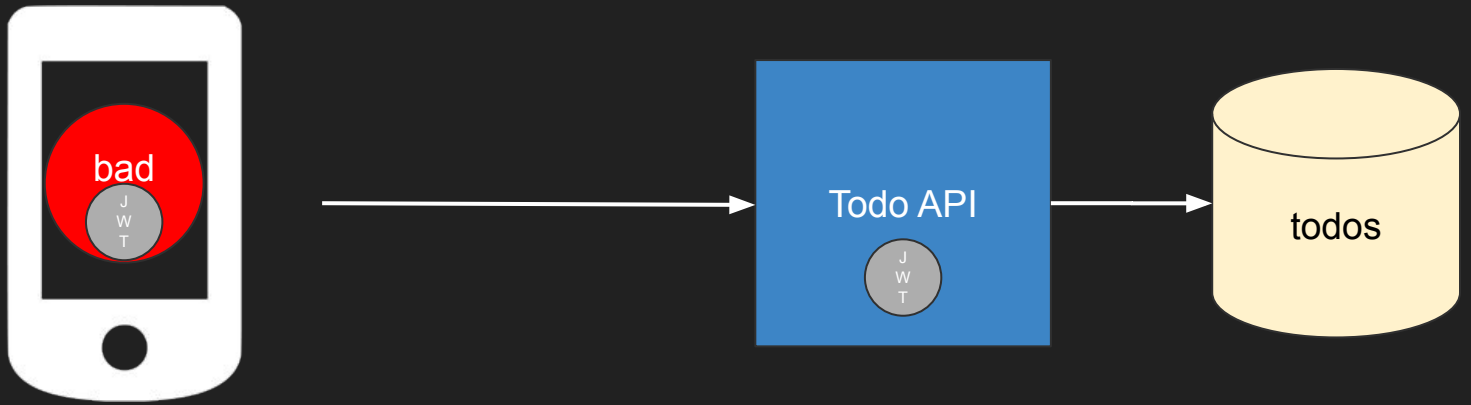
FusionAuth

JWT Footguns

- Lots of configuration options
  - Use a library
  - Verify your claims
- Can contain arbitrary JSON data
  - No secrets
  - Contents are base 64 decoded
- HMAC key length

JWT Footguns (pt 2)

- Store carefully when an access token


bad
J
W
T
Todo API
J
W
T
todos

Token storage

- Prefer server side
- HttpOnly cookie on browser
  - Watch out for XSS
- Secure storage on mobile

The “None” Signing Algorithm

JWT Footguns (pt 3)

- JWT specification allows a “none” algorithm
  - No signature is required

JWT

eyJhbGciOiJSUzI1NiJ9.eyJpc3MiOiJmdXNpb25hdXRoLmlvIiwiZXhwIjoxNTg5MjI3MDA2LCJhdWQiOiIyMzhkNDc5My03MGRlLTQxODMtOTcwNy00OGVkOGVjZDE5ZDkiLCJzdWIiOiIxOTAxNmI3My0zZmZhLTRiMjYtODBkOC1hYTkyODc3Mzg2NzciLCJuYW1lIjoiRGFuIE1vb3JlIiwicm9sZXMiOlsiUkVUUklFVkVfVE9ET1MiXX0.dlXJ3bdjsN9ivekeYMJdeA5jla6cKqxTkBixijRDpSTdDwwtSX4j0MdBsQhrYnJqVRdtBAufRC3T5hQpKVPgskP1nfkRqSJx1awZajeinab76HD_mdm5RwtuXycBgJ9KJt3JPAkyLSpeT-SrWO1h2gLt4pioP8GtSpIZocEXMcKkeOL7-8KyZAi1VYYQN3aiy0ZkbaKq7_nj2SrMYw4myRaAIYj0Ngamx9DlZrVfmSM4xn6ZwcvT17y_Ff0VX9T-Z6x9dEIPxhi8EVBDzyclmhaULn_9ALp2oIIIdACqzgoGZc2MwC0DED7-IIRt0Qi20H9nfyGavfDs80aGcubVLQ

JWT

eyJhbGciOiJub25lIn0.eyJpc3MiOiJmdXNpb25hdXRoLmlvIiwiZXhwIjoxNTg5MjI3NDgwLCJhdWQiOiIyMzhkNDc5My03MGRlLTQxODMtOTcwNy00OGVkOGVjZDE5ZDkiLCJzdWIiOiIxOTAxNmI3My0zZmZhLTRiMjYtODBkOC1hYTkyODc3Mzg2NzciLCJuYW1lIjoiRGFuIE1vb3JlIiwicm9sZXMiOlsiUkVUUklFVkVfVE9ET1MiXX0.

JWT Header

```
eyJhbGciOiJSUzI1NiJ9
```

=

```
{
   "alg": "HS256"
}
```

JWT Header

```
eyJhbGciOiJub25lIn0
```

=

```
{
  "alg": "none"
}
```

JWT

eyJhbGciOiJub25lIn0.eyJpc3MiOiJmdXNpb25hdXRoLmlvIiwiZXhwIjoxNTg5MjI3NDgwLCJhdWQiOiIyMzhkNDc5My03MGRlLTQxODMtOTcwNy00OGVkOGVjZDE5ZDkiLCJzdWIiOiIxOTAxNmI3My0zZmZhLTRiMjYtODBkOC1hYTkyODc3Mzg2NzciLCJuYW1lIjoiRGFuIE1vb3JlIiwicm9sZXMiOlsiUkVUUklFVkVfVE9ET1MiXX0.

JWT Specification Allows This!

Simple Fix = Don’t Allow “none”

EVER!

Unless you have some other way to verify the JWT is unchanged

Unless you have some other way to verify the JWT is unchanged

Mutual TLS

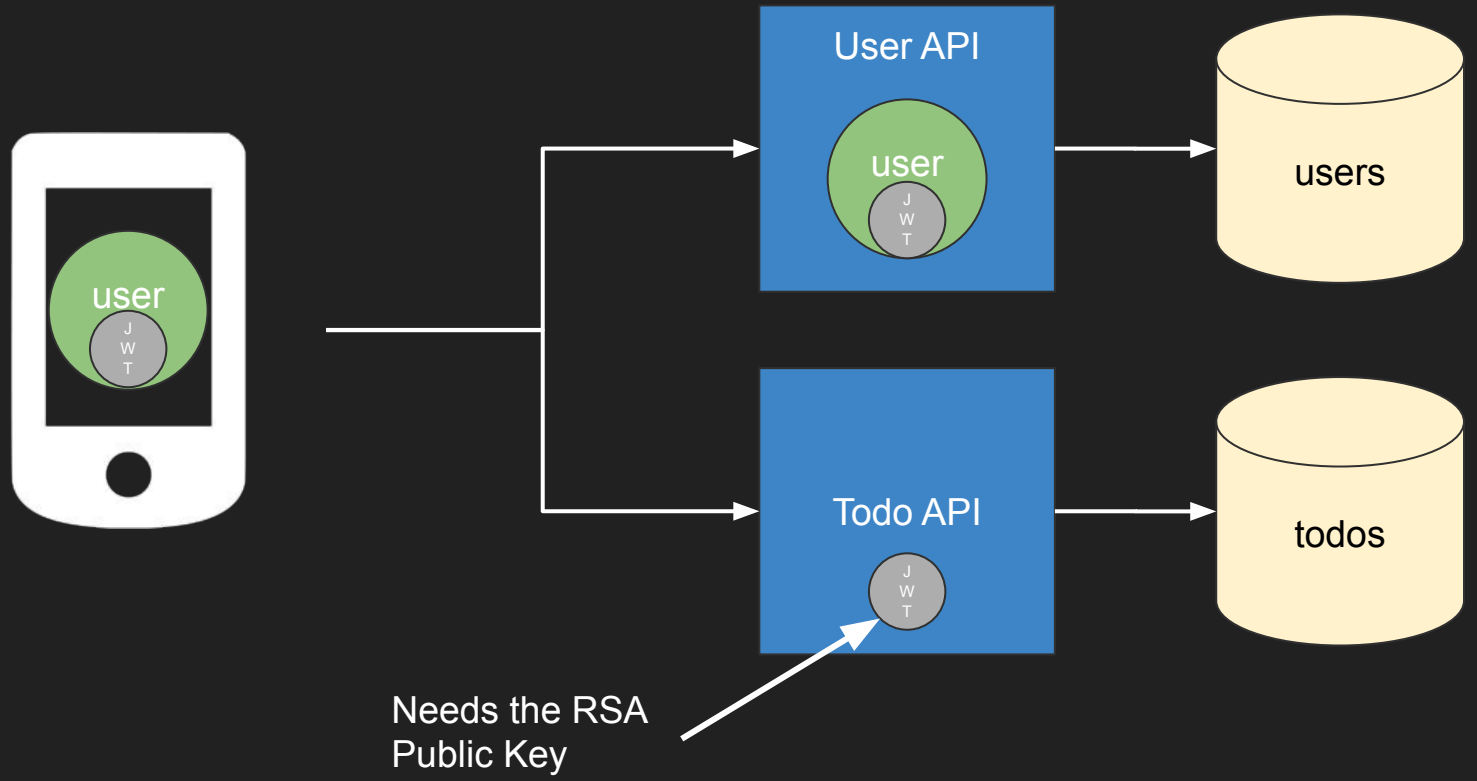
Signing With Public Private Key Pairs

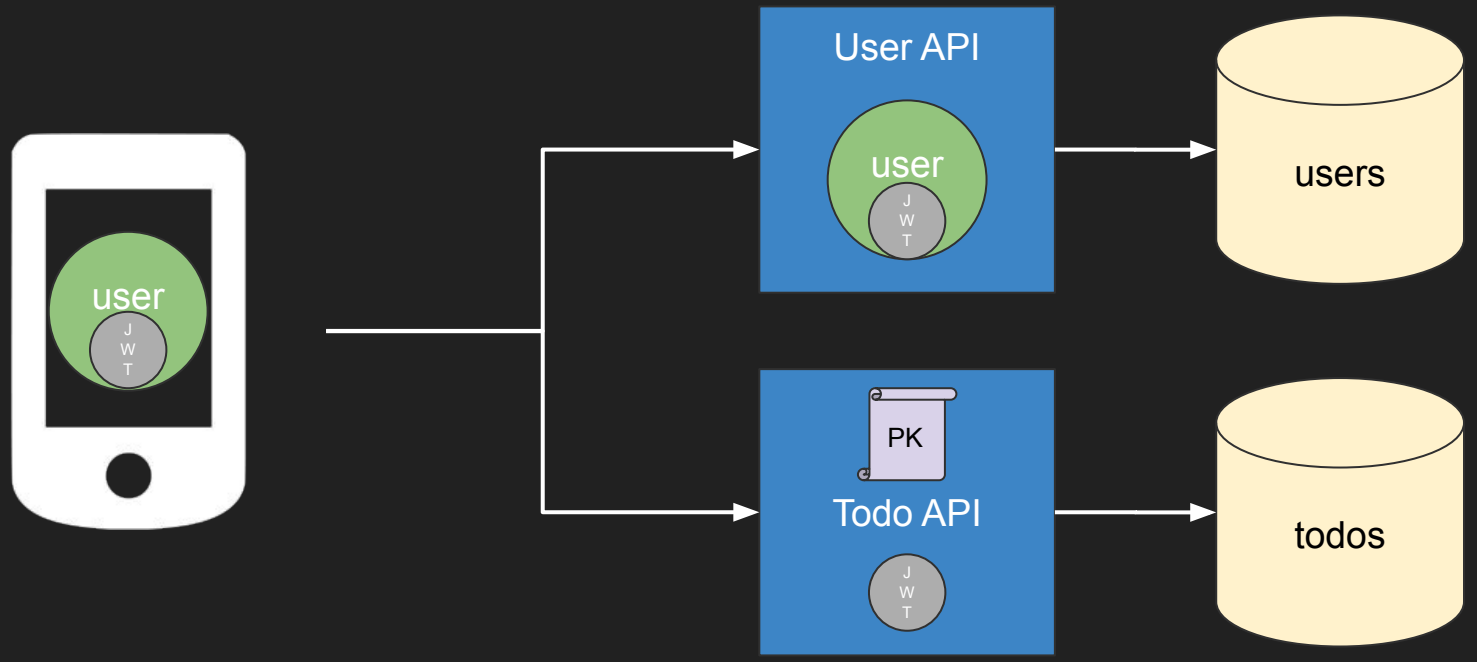
Why?

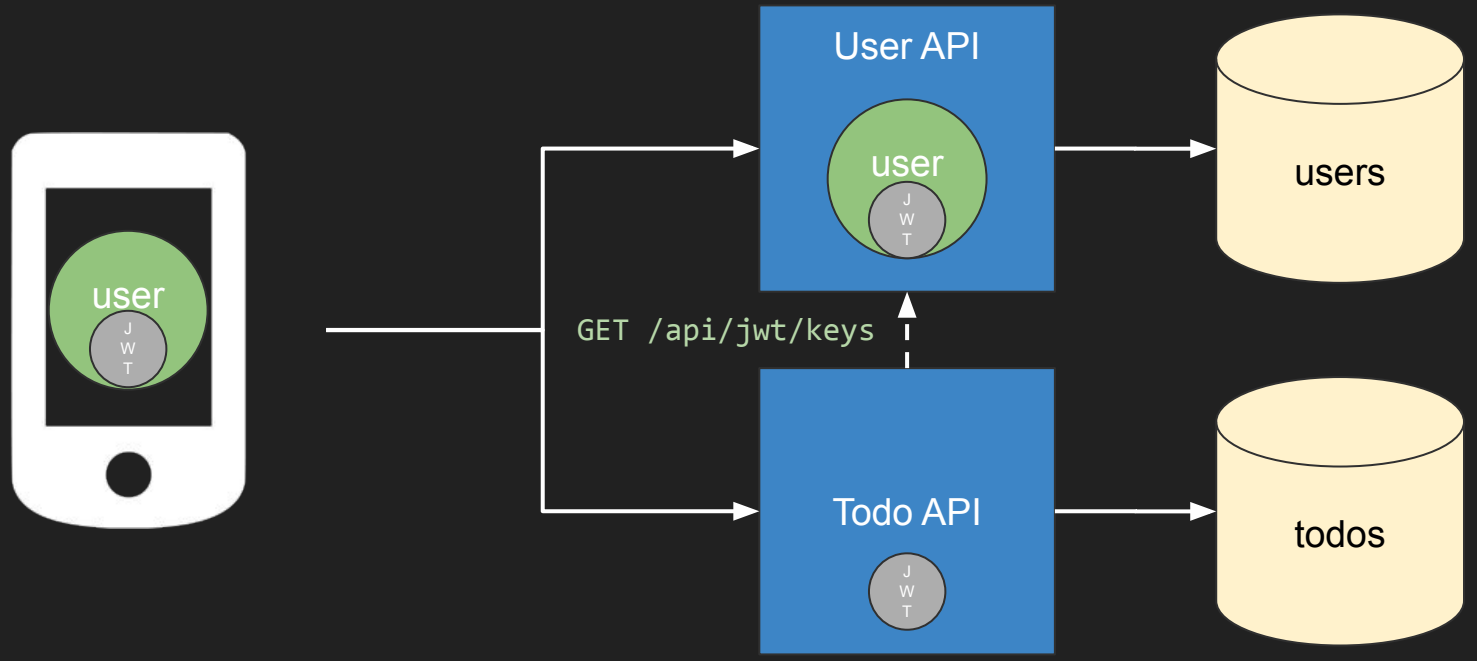
- No shared secret
  - Scales organizationally
  - Security
- Key rotation easier
  - Support multiple keys

TANSTAAFL

- More complicated
- Slower


user
J
W
T
User API
user
J
W
T
users
Todo API
J
W
T
todos
Needs the RSA
Public Key


user
J
W
T
User API
user
J
W
T
users
PK
Todo API
J
W
T
todos


User API
user
J
W
T
users
user
J
W
T
GET /api/jwt/keys
Todo API
J
W
T
todos

```
{
  "publicKey": "-----BEGIN PUBLIC
KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEArPvW9SEPuzi2Mg5FTTN8Y\
nLr0VOBzvX1O7U9Ee0+8+2Xvv3GeLMxquJ7Ijn
osV0fdoZmqrjXwA++ipqKHuhWk/b\nPsjXWijE
/a0q0yTn3f ..."
}
```

Multiple Keys?

JWT Header

```
{
  "typ": "JWT",
  "alg": "RS256",
  "kid": "42"
}
```

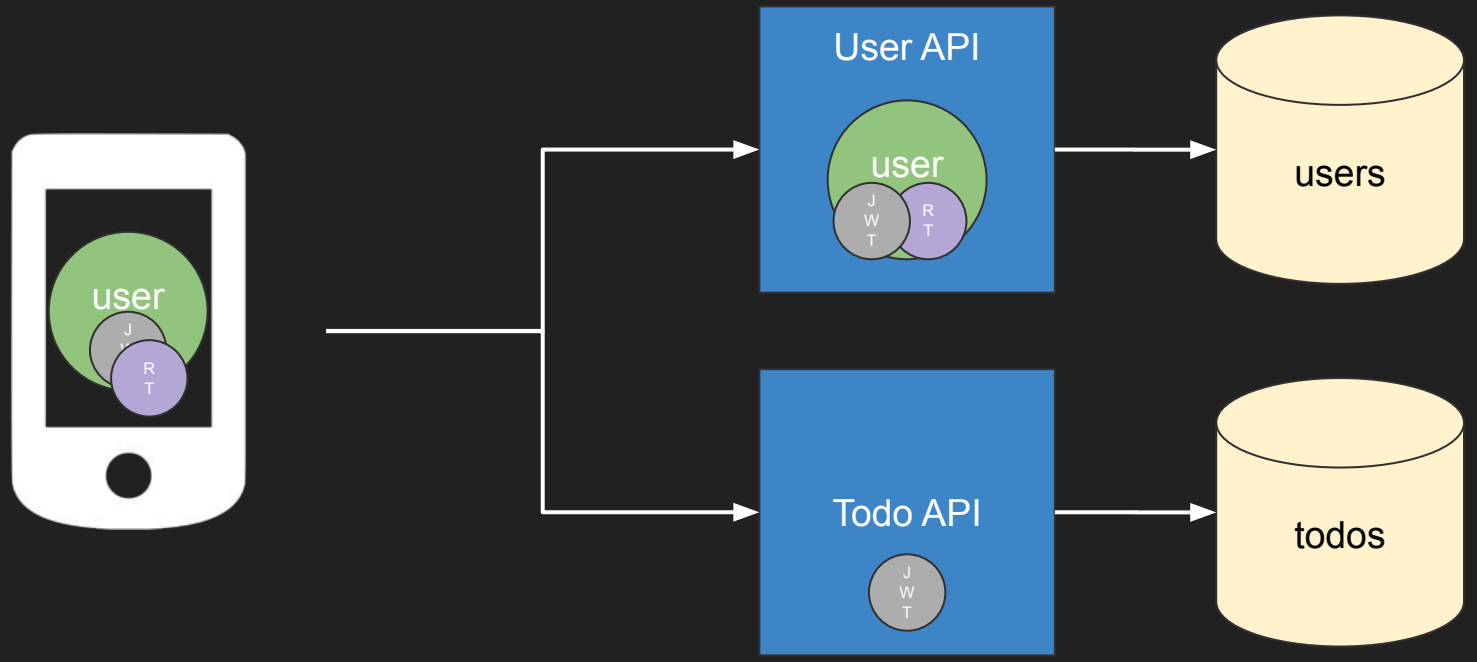
```
{
  "publicKeys": {
    "42": "-----BEGIN PUBLIC
KEY-----\nMIIBIjANBgkqhkiG9w0BAQEFAAOC
AQ8AMIIBCgKCAQEArPvW9SEPuzi2Mg5FTTN8Y\
nLr0VOBzvX1O7U9Ee0+8+2Xvv3GeLMxquJ7Ijn
osV0fdoZmqrjXwA++ipqKHuhWk/b\nPsjXWijE
/a0q0yTn3f ..."
  }
}
```

Refresh Tokens

- JWTs are meant to be short lived (minutes)
- Refresh tokens are long lived (days or months)
- Refresh tokens can be used to create new JWTs

Why Refresh Tokens

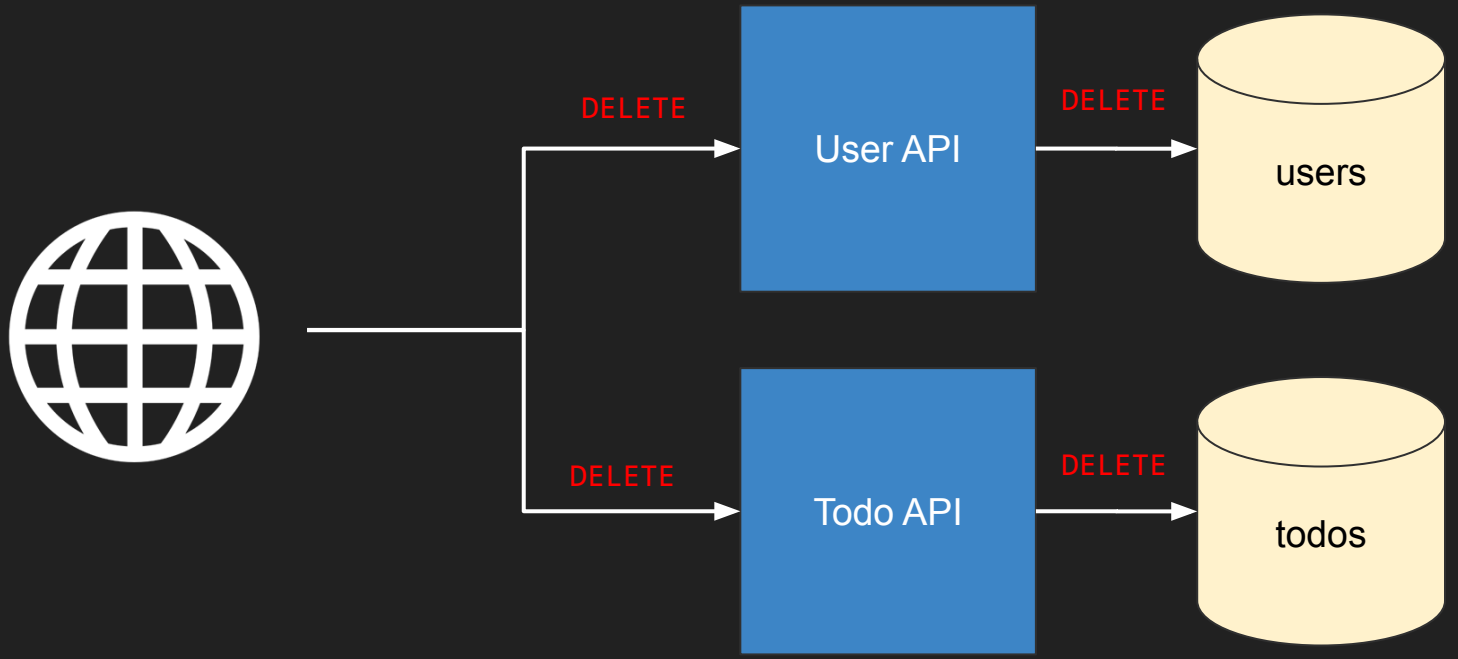
- Compromise between
  - User authenticating regularly
    - User hassle
  - Long lived JWTs
    - Security risk

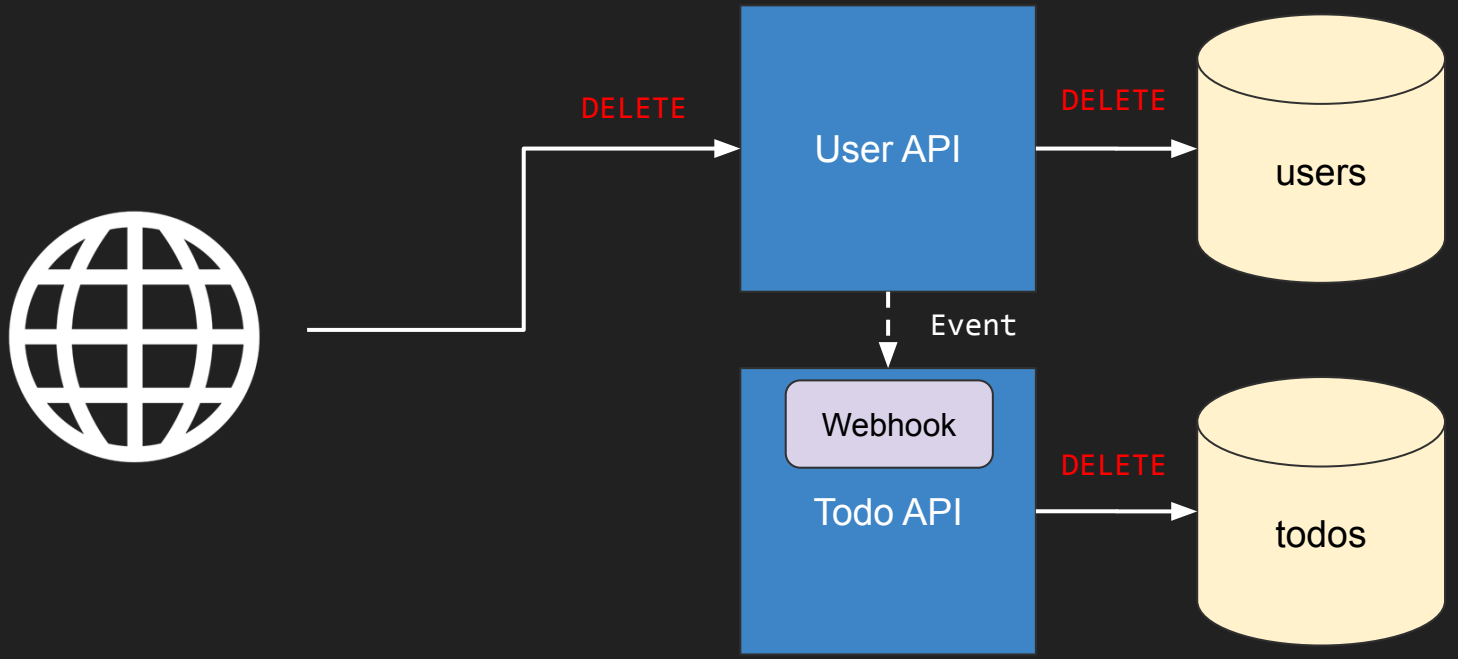

user
J
R
T
User API
user
J
W
T
R
T
users
Todo API
J
W
T
todos

Deleting Users?

```
delete from users where user_id = 42
        on delete cascade;
```

Oops! No ON DELETE CASCADE


DELETE
User API
DELETE
users
DELETE
Todo API
DELETE
todos

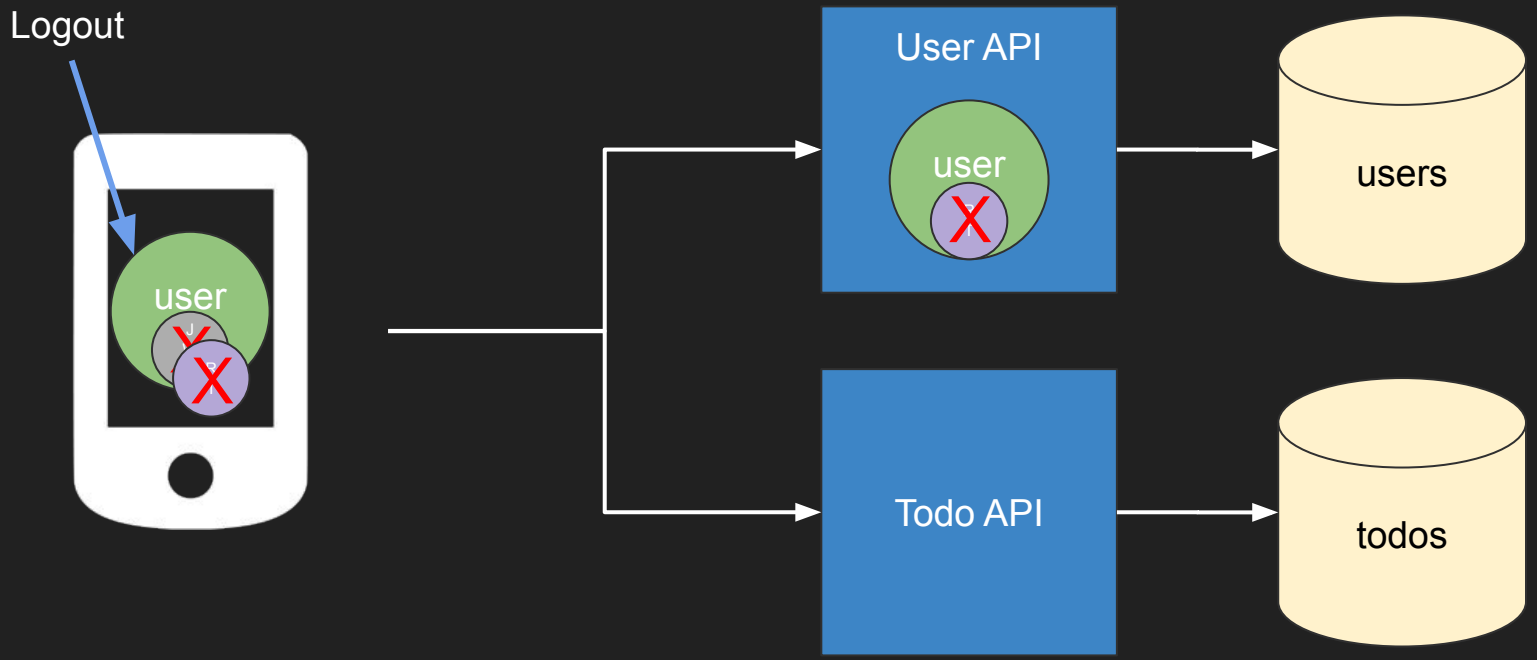

DELETE
User API
DELETE
users
Event
Webhook
Todo API
DELETE
todos

Logout (aka Revocation)

- Revoke the refresh token

`/api/logout`

NOT


Logout
user
User API
user
users
Todo API
todos

Global Logout/Revoke

Make sure you can logout of everything or revoke all refresh tokens.

Can I Revoke JWTs?

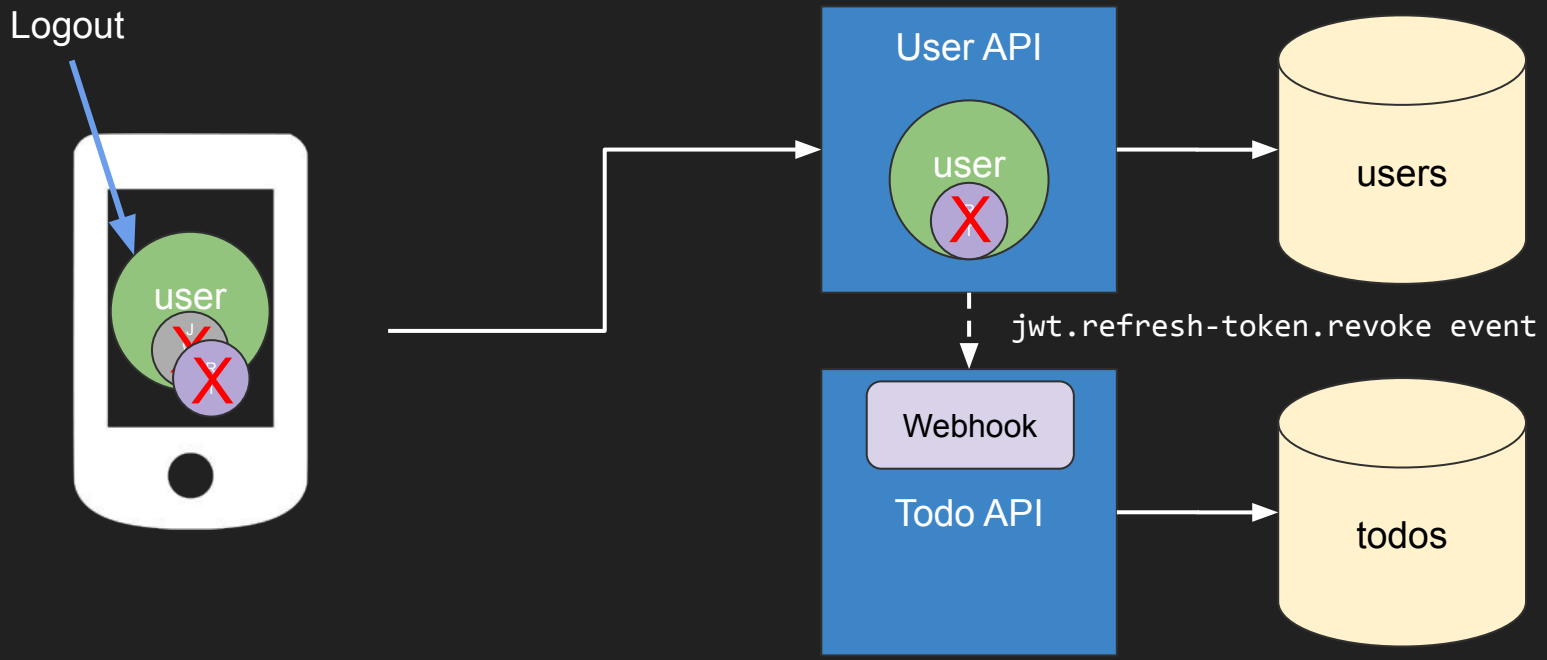
Sorta

Let’s say a user’s account has been breached

Rotate keys


SOME PEOPLE
JUST WANT TO WATCH THE WORLD BURN
quickmeme.com

Time window solution


Logout
user
User API
user
users
jwt.refresh-token.revoke event
Webhook
Todo API
todos

Right now it’s

Dec 9th, 2020 1:12:47 pm

A new JWT created right now will expire at:

Dec 9th, 2020 1:42:47 pm

A JWT created one second ago will expire at:

Dec 9th, 2020 1:42:46 pm

Therefore, all JWTs that expire on or before:

Dec 9th, 2020 1:42:46 pm

are invalid!

1:12:47 pm

1:42:47 pm

@mooreds

FusionAuth

Code!

JWTs + Rails

- What are you trying to accomplish?
  - Generate/parse JWTs - use ‘jwt’ gem
    - lib/jwt/default_options.rb
  - Authorization
    - Before filter / JWT
    - https://github.com/waiting-for-dev/devise-jwt
    - https://github.com/nsarno/knock

JWT Tools

- https://fusionauth.io/learn/expert-advice/dev-tools/jwt-debugger
- https://github.com/FusionAuth/fusionauth-example-ruby-jwt
- https://fusionauth.io/learn/expert-advice/tokens/building-a-secure-jwt

Thanks / Contact

- To You!

- Contact
  - dan@fusionauth.io
  - FusionAuth.io
  - @mooreds