JSON Web Token je standard za bezbedno prenošenje informacija između dve strane. Podrazumeva digitalni potpis, pa je informacija proverena i može joj se verovati.

JSW je kompaktan: može se poslati kroz URL, POST, HTTP header.

Jedan token sadži sve potrebne informacije u sebi. Sadrži informaciju o korisniku, pa se time omogućava da nije neophodno dodatno komunicirati sa bazom (jednom se uloguje korisnik).

JWT je koristan za autentikaciju i razmenu informaciju.

Kako izgleda JWT?

aaaaaaaa.bbbbbbbbbbbbb.ccccccccc

Na primer:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJsb2dnZWRJbkFzIjoiYWRtaW4iLCJpYXQiOjE0MjI3Nzk2Mzh9.gzSraSYS8EXBxLN\_oWnFSRgCzcmJmMjLiuyu5CSpyHI

**header.payload.signature**

**Header:**

{

“alg”: “HS256”,

“typ”: “JWT”

}

Algoritam kojim je kodiran

Header se kodira pomoću Base64Url i dobije se niska aaaaaaaaaa tj. header (pre prve tacke)

**Payload**:

{

“sub”: “1234567890”,

“name”: “John Doe”,

“admin”: true

}

Podaci o korisniku, i dodatni metapodaci (npr. rok trajanja tokena).

Base64Url -> bbbbbbbbbbbbbb

*Kako da znamo da nisu podaci promenjeni tokom transfera?*

**Signature:**

HMACSHA256(

Base64UrlEncode(header) + '.' +

Base64UrlEncode(payload),

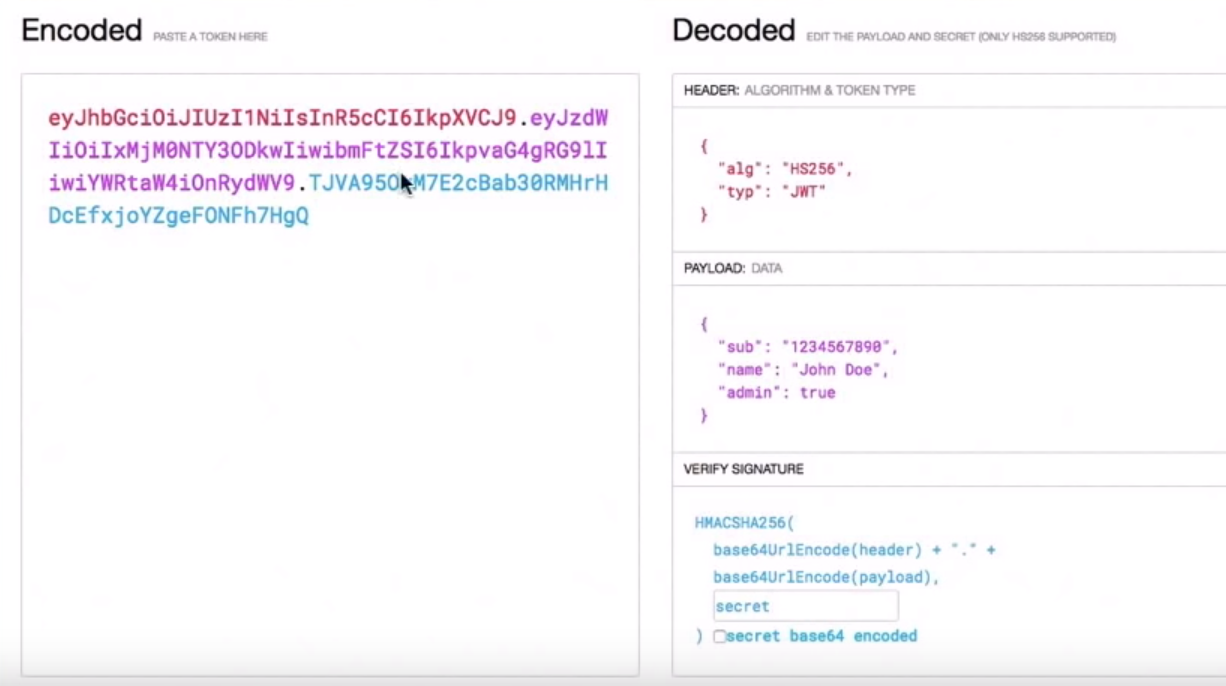
secret

)

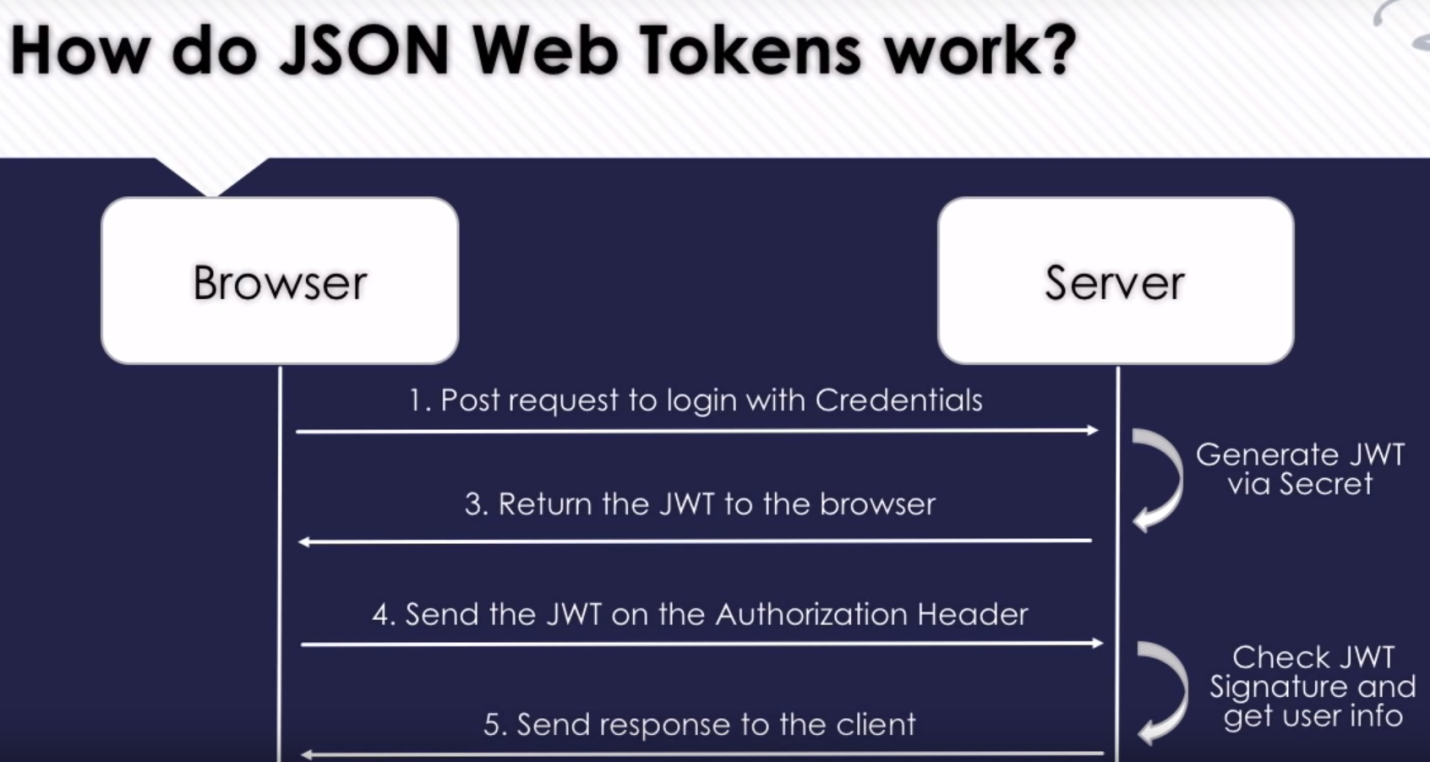
Kriptografski algoritam naveden u header-u.

Base64Url -> ccccccccccccccc

Ova tri dela se nadovežu sa tačkama između.



Iz pregledača (engl. *Browser*) se šalje POST zahtev serveru sa podacima za logovanje. Server to proverava i ukoliko je sve u redu JWT se generiše sa tajnom (Secret). JWT se vraća pregledaču. Ukoliko je JWT u redu, šalje se serveru da se pristupi nekim delovima veb sajta. Onda se na serveru proveri JWT potpis i šalje odgovor korisniku.



<https://jwt.io/>

<https://www.base64decode.org/>

**REST** (REpresentational State Transfer) je koncept organizacije podataka preko interneta. Najčešće se koristi JSON format.

**API** (Application Programming Interface) je skup pravila koji omogućavaju da jedan softver komunicira sa drugim. Ova pravila mogu uključivati operacije: create, read, update i delete.

HTTP Request Methods:

GET – da se dobiju podaci od API-a

POST – da se posalje podatak u API, ali ne mogu se podaci staviti u telo POST naredbe (za to nam treba Postman REST client)