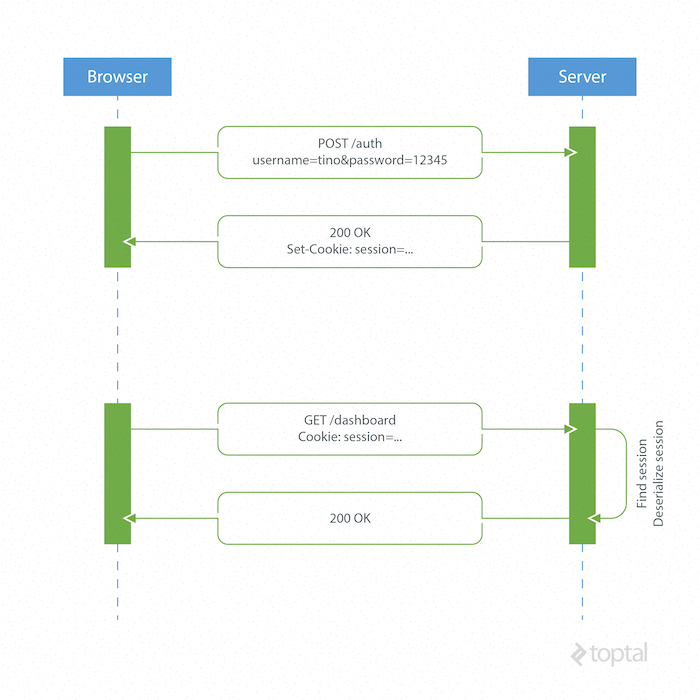
**What is a JWT Token?**

* URL Safe.
  + Characters that are allowed in a URI. These include uppercase and lowercase letters, decimal digits, hyphen, period, underscore, and tilde.
* A JWT is digitally signed,
  + Meaning it uses SHA algorithm to encrypt payload.
  + Provides integrity of the payload. i.e if data is modified on the way, server identifies it easily.
* OAuth2 uses JWT as OAuth2 Access Tokens.

**Disadvantage of JWT**

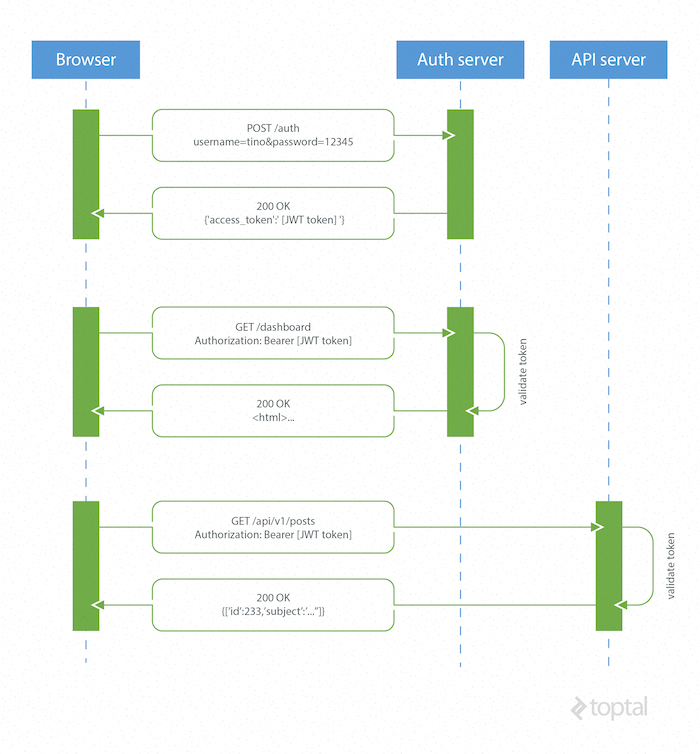
Whoever has the JWT token can access the resource. But generally we use TLS-i.e HTTPS so no one can see this token.

**Traditional State Maintenance Approach**



1. Application Server manages the session logic or session logic is tightly coupled with application.

**Token Based Authentication**



* This removes the authentication and authorization burden of Application Server to Authorization Server.

**How JSON Web Tokens Work**

* A browser or mobile client makes a request to the authentication server containing user login information.
* The authentication server generates a new JWT access token and returns it to the client.
* On every request to a restricted resource, the client sends the access token in the query string or Authorization header.
* The API server then validates the token and, if it’s valid, returns the secure resource to the client.
* The authentication server can sign the token using any secure signature method. For example, a symmetric key algorithm such as HMAC SHA-256 can be used if there is a secure channel to share the secret key among all parties.
* Alternatively, an asymmetric, public-key system, such as RSA, can be used as well, eliminating the need for further key-sharing.

**How does JWT looks like**



eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.

eyJpc3MiOiJ0b3B0YWwuY29tIiwiZXhwIjoxNDI2NDIwODAwLCJodHRwOi8vdG9.

yRQYnWzskCZUxPwaQupWkiUzKELZ49eM7oWxAQK\_ZXw