# Token based authentication

Cookies + session authentication

* Cookies set on the client side by the server
* Cookies used as a storage for session ID that is used as an index into server-side storage of session information

Why token-based authentication?

* Session authentication becomes a problem when we need stateless servers and scalability
* Mobile application platforms have a hard time handling cookies/sessions
* Sharing authentication w other applications not feasible
* Cross-origin resource sharing problem (CORS)
* Cross-site request forgery (CSRF)

How does it work

1. User requests access w username and password
2. Server validates credentials
3. Server creates a signed token and sends it to the client
   1. Nothing stored on the server
4. All subsequent requests from the client should include the token
5. Server verifies the token and responds w data if validated

JSON web tokens (JWT)

* Standards based
  + IETF RFC 7519
* Self-contained
  + Carry all the information necessary within itself
* Shareable
  + Can share it w other applications to act on your behalf