Most used authentication methods

Session Cookies

* Small piece of data stored both on server and client
* Usually, server stores the session information in the database or in-memory storage
* In the client cookies are manages by a browser. They are included in every request.
* Stateful elements
* Each session contains unique identifier used by server to identify the current user and all the data associated with that user.
* Share the information between domains and sub-domains
* Share with other domain is not possible
* To restrict client site JavaScript manipulation, you can use the “HTTP Only” flag
* Cookies are only secure with HTTPS connections. For this “secure” flag can be used to ensure cookies sent only in HTTPS connections

Tokens

* Tokens are set of character or numbers
* Tokens are stateless
* Server doesn’t have to store any information regarding the token
* Tokens are self-contained (Information required for verification on server is stored inside the token)
* Suitable for API authentication because no database lookups are required.
* Tokens are flexible and used for multi-platform applications
* We can share tokens between different domains