# **Authorization and CORS**

## 1.1 Authorization header

The Authorization HTTP header provides authentication information on a request. There are several types of authentication that use this header, and some are supported by browsers, such as [basic authentication](https://en.wikipedia.org/wiki/Basic_access_authentication). When an unauthenticated request is received by the server, it will respond with a HTTP 401 Unauthorized response with a WWW-Authenticate header. This will trigger the browser to ask the user for credentials.

## 1.2 CORS

The CORS mechanism supports secure cross-origin requests and data transfers between browsers and servers. Modern browsers use CORS in APIs to mitigate the risks of cross-origin HTTP requests. The Cross-Origin Resource Sharing standard works by adding new [HTTP headers](https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers) that let servers describe which origins are permitted to read that information from a web browser. Additionally, for HTTP request methods that can cause side-effects on server. Servers can also inform clients whether "credentials" (such as [Cookies](https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies) and [HTTP Authentication](https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication)) should be sent with requests.