**What is API Response?**

**Every API request is associated with response. The response have 2 facets**

**1. Status code : Numeric representation of the web server response. There are pre-defined set of status code which can be reused. Or, teams can create their own status code as per convenience. However, appropriate status code range should be used.**

**2. Status Message : Each status code is associated with detailed response message.**

**for example:**

**Status code 200 → Success**

**Status code 401 → Unauthorized**

**Status code 404 → Not found**

**What is API Gateway?**

**API gateway helps establishing authentication to verify the calls before transferring it to further execution. The capability of API gateway is not just restricted to authentication, it also provides multitude of services like**

**I. Routing**

**ii. Rate Limiting**

**iii. Analytics**

**iv. Security**

**v. Policies etc**

**API Authentication:**

**Authentication is a process of verifying the identity of the user it solely answers who you are, whereas authorisation mostly deals with access management and comes into play only after the user is identified and verified successfully.**

**1.Basic Authentication:**

**This technique involve providing username and password for user verification. When user enters their credentials the details are encoded in Base64 generating a Key which will be bundled in request header and sent to server for verification. Server Verifies the key with the stored username and password. If the identity is verified the request is fulfilled else an error is sent back denying request sent.**

2. API Key Authentication:

**API key is a long encrypted string which identifies the application without any principal. These are sent either as a part of request header or URL. When client recognises the API key server will process the request.**

**3.OAUTH Authentication:**

**This technique is considered quite powerful and secure way of authenticating the users. OAuth technique can also be used for authorisation. Initially a user may have to login to the OAuth application using the credentials to generate a token. The generated token is attached as part of request header, which will be sent to authentication server in order to verify. If the token is recognised the API request will be processed.**