**Tokenization Authentication**

**Tokenization Authentication -**

* Tokenization Authentication is a method where a token is used to authenticate a user instead of methods like a username and password.
* Token is usually obtained by logging in once that can be used for requests
* it is secure
* When the user login using their username and password
* The server verifies the credentials and if correct generates a token
* This token is sent back to the user
* The user uses this token to authenticate the requests
* The Token included in the headers of the requests
* The server verifies the token to ensure its valid or not
* If we have a token then we don't need to send our username and password with every request
* Token are typically included in the “Authorization” header with the “Bearer” prefix
* Tokenization helps ins securely communicating with APIs

**Types of Tokens:**

1. **API keys :** API keys is a simple token used to identify the calling user
2. **Bearer Tokens:**This Token represent the users authorization to access resources
3. **JWT (JSON web Tokens) :** Tokens that carry information about the user and are used to verify identity

**How Tokenization works :**

1. **Using Tokens in Requests:**

1. In Headers: We Go to the “Headers” tab and add new header with the key “Authorization” and value “Bearer {access token}

2.In URL Parameters : Add The token directly in the URL as a Query parameter

3. In Request body : Add the token in the body of our request for POST requests

1. **Storing Tokens:**

Tokens can be stored in postman’s environment variables. This makes it easy to use them across multiple request