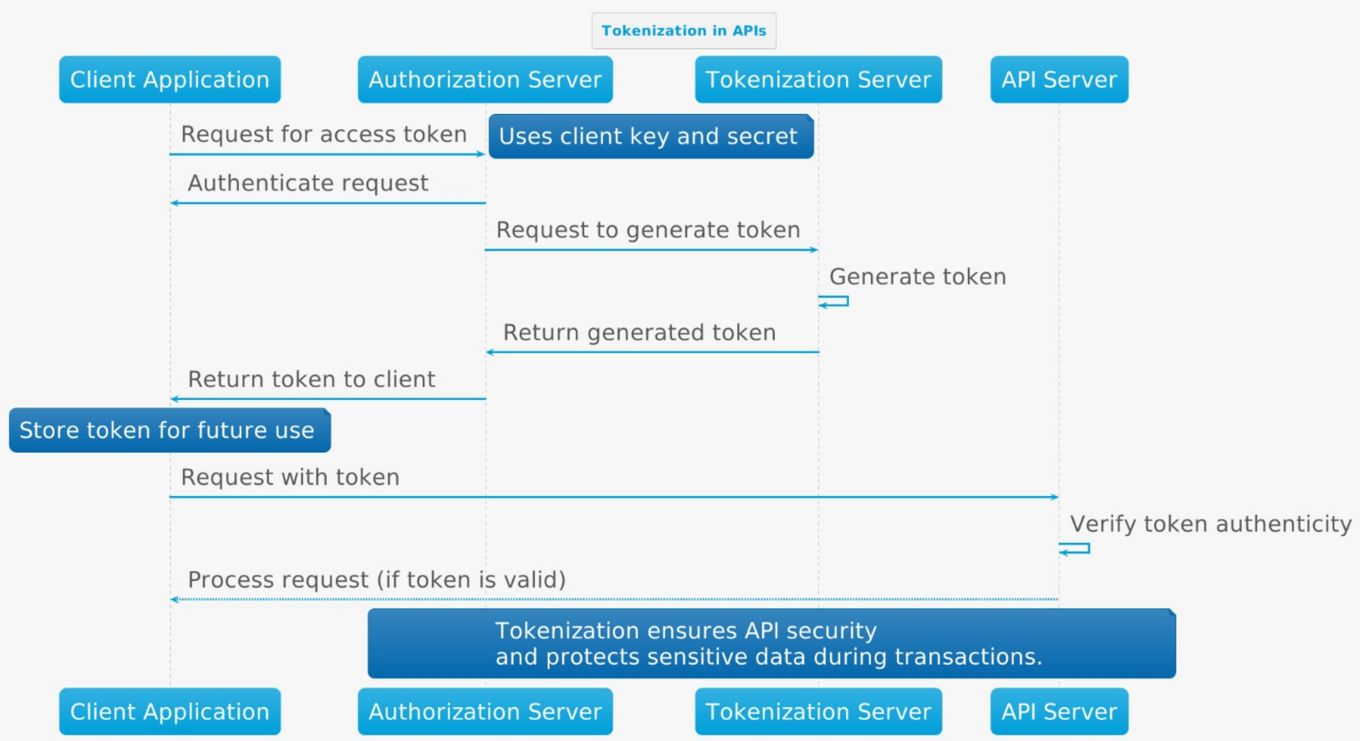
SDE Lab 03: REST ADVANCED

DOCUMENTATION: Tokenization In APIs

Tokenization in APIs

Tokenization in context of APIs typically refers to the process of generation and managing tokens that are used for authentication and authorization. These tokens are often used to secure API endpoints and control access to resources.

How do tokenization work in APIs?



1. **Authentication**: When client wants to access an API, it needs to provide its identity. This is typically done using the combination of a user name and password or some other form of a credentials. Once the client's identity is verified the API server generates a token.
2. **Token Generation**: The token is a random string or a unique identifier that represents the clients authenticated session. It is generated by the API server and is associated with a specific user or client.
3. **Token Storage**: The generated token is then usually stored on the client side (e.g. in a cookie, a local storage or a mobile app's memory). It is crucial to protect this token because it serves as a proof of authentication. If it fails into the wrong hands unauthorized access can occur.
4. **Authorization**: In addition to authentication, tokens can also carry information about what the client is authorized to do. This information is embedded in the token, and the API server can use it to determine which resources and the actions the clients is allowed to access.
5. **Token Expiration and Refresh**: Tokens often have a limited lifespan to enhance security. After a token expires, the client needs to request a new token. Refresh tokens can be used to obtain new access tokens without requiring the user to re-enter their credentials.
6. **Token Usage**: When the client makes a request to the API, it includes the token in the request header. The API server checks the token to ensure the client is authenticated and authorized to perform the

requested action.
7. **Token Revocation**: In case a token in Compromised or no longer needed, it can be revoked by the API server. Revoked tokens are no longer valid for authentication.

Tokens can take different forms, including JSON Web Tokens (JWT), OAuth 2. 0 access tokens, API keys and more. The choice of token format and authentication method depends on the specific use case and the security requirements of the API.

In our case, we are focusing with the API keys. As you are familiar now, in order to get your API keys, you had to sign up in Rapid API, that is an example of Authentication, and the unique API key you got is what the token generation is and it is generated by API server. And with the API key related to Jokes, you are authorized to generate random jokes with only 10 request per hour, this is authorization.