**Theory: Authentication and Authorization API**

**Authentication vs. Authorization**

1. **Authentication**:
   * **What it is**: Authentication is the process of verifying the identity of a user or system. It ensures that the entity (user, device, etc.) is who they claim to be.
   * **Example**: When you log into a website with your username and password, the system authenticates that you are who you say you are.
2. **Authorization**:
   * **What it is**: Authorization, on the other hand, determines what actions or resources the authenticated user is allowed to access. It checks if the authenticated user has permission to perform certain actions.
   * **Example**: Once you're logged in, your permissions (e.g., "Can edit profile" or "Can view dashboard") are verified through authorization.

**Authentication Methods in Django REST Framework (DRF)**

Django REST Framework provides several authentication methods, including:

* **Token Authentication**: A simple method where the server issues a token when a user logs in. This token is then sent with subsequent requests to authenticate the user.
* **Session Authentication**: Uses Django's built-in session management (cookies) to maintain the authenticated user's state.
* **OAuth2 Authentication**: Used for third-party authentication (e.g., Google, Facebook logins).