JWT Authentication and Connected App in Salesforce

🔓 What is JWT (JSON Web Token)?

A secure, compact, and URL-safe token used to represent claims between two systems.

- It enablies sener-to-server authentication **without** user interaction
- A GitHub worktlow (like GitHub Actions) generates a JWT using a prhe key
- This JWT is sent to Salesforce's token endpoint
- Salesforce validates the JWT using a *public key* stored in a Connected App
- If the token is valid, Salesforce issues an access token for API calls

What is a Connected App in Salesforce?

A Connected App is how external system, like GitHub, securely authenticate and interact with Salesforce.

1. Create a Connected App in Salesforce Setup.
2. Enable OAuth Settings:

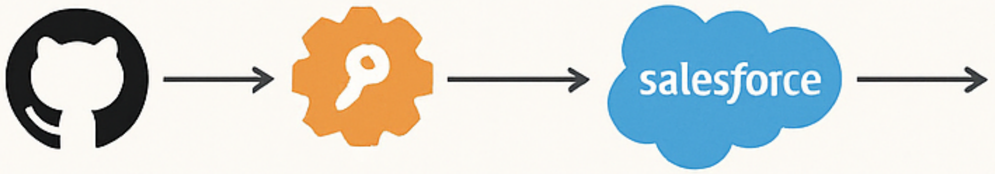
   ✓ Check "Use digital signatures" (from the private oky in GitHub)

   🌐 Set a callback URL (optional for JWT flows)

   🔒 Add required OAuth Scopes, e.g.:

   - Full access (fuil)
   - Perform requests on your behalf at any time (refresh_token, offline_access)
3. After saving, note the Consumer Key — this is used by GitHub when generating the JWT

Flow Summary



1. GitHub signs a JWT using its private key.
2. The JWT is sent to Salesforce's OAuth ttoken endpoint.
3. Salesforce valldates it against the public key uploaded in he Connected App.
4. If valid, Salesforce returns an access token.