ONE PAGE SUMMARY

IT & Software › API Development › Authentication for APIs

Introduction to Authentication for APIs

Secure your APIs with effective authentication methods.

DEFINITION

> Authentication for APIs is the process of verifying the identity of users or systems accessing an API. It ensures that only authorized entities can interact with the API's resources.

KEY CONCEPTS

API Key

A unique identifier used to authenticate a user or application when making API requests.

OAuth 2.0

A widely used authorization framework that allows third-party applications to access user data without sharing passwords.

JWT (JSON Web Token)

A compact, URL-safe means of representing claims to be transferred between two parties, often used for authentication.

Basic Authentication

A simple authentication scheme built into the HTTP protocol, where credentials are sent as a base64-encoded string.

Token Expiration

A security measure where tokens are set to expire after a certain period, requiring re-authentication.

EXAMPLES

→ Using an API key to access a weather data service.

→ Implementing OAuth 2.0 for a social media login feature.

→ Verifying user identity with JWT in a mobile app.

MEMORY TIPS

★ Remember 'API Key' as 'Access Permission Identifier'.

★ Think of OAuth as 'Open Authorization' for third-party access.

★ JWT can be recalled as 'Just Verify Token'.

COMMON MISTAKES

✗ Neglecting to secure API keys in source code.

✗ Using weak passwords for Basic Authentication.

✗ Not implementing token expiration for security.

QUICK RECAP

Authentication for APIs ensures that only authorized users can access resources. Key methods include API keys, OAuth 2.0, and JWT. Always secure your credentials and implement token expiration.