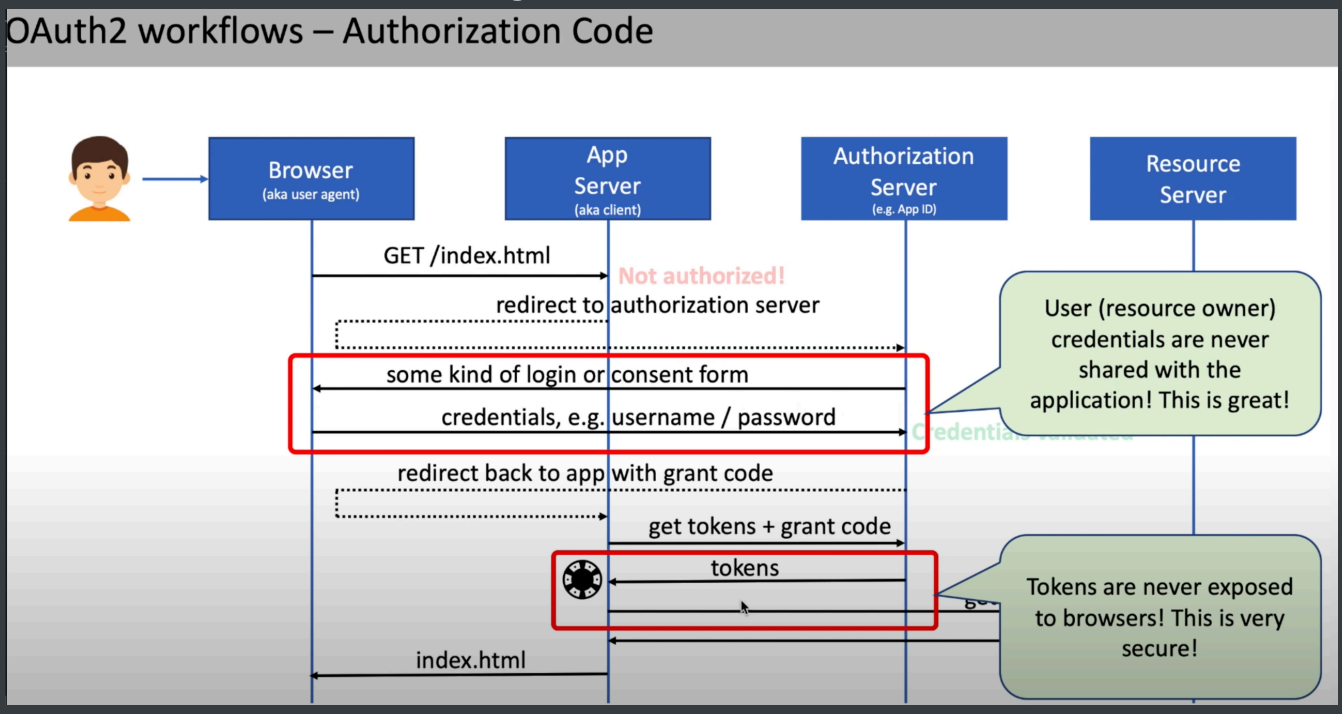
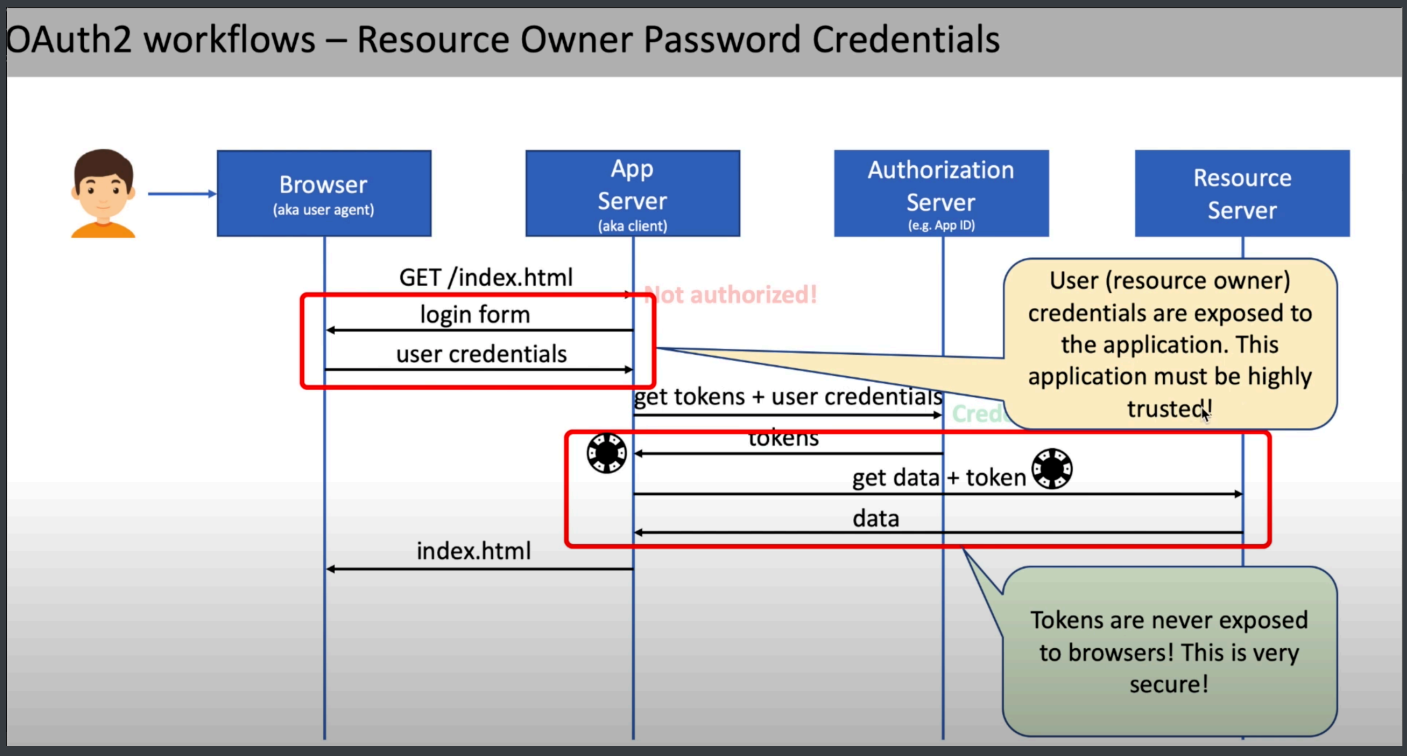
Access token（based on OAuth2）

main workflows

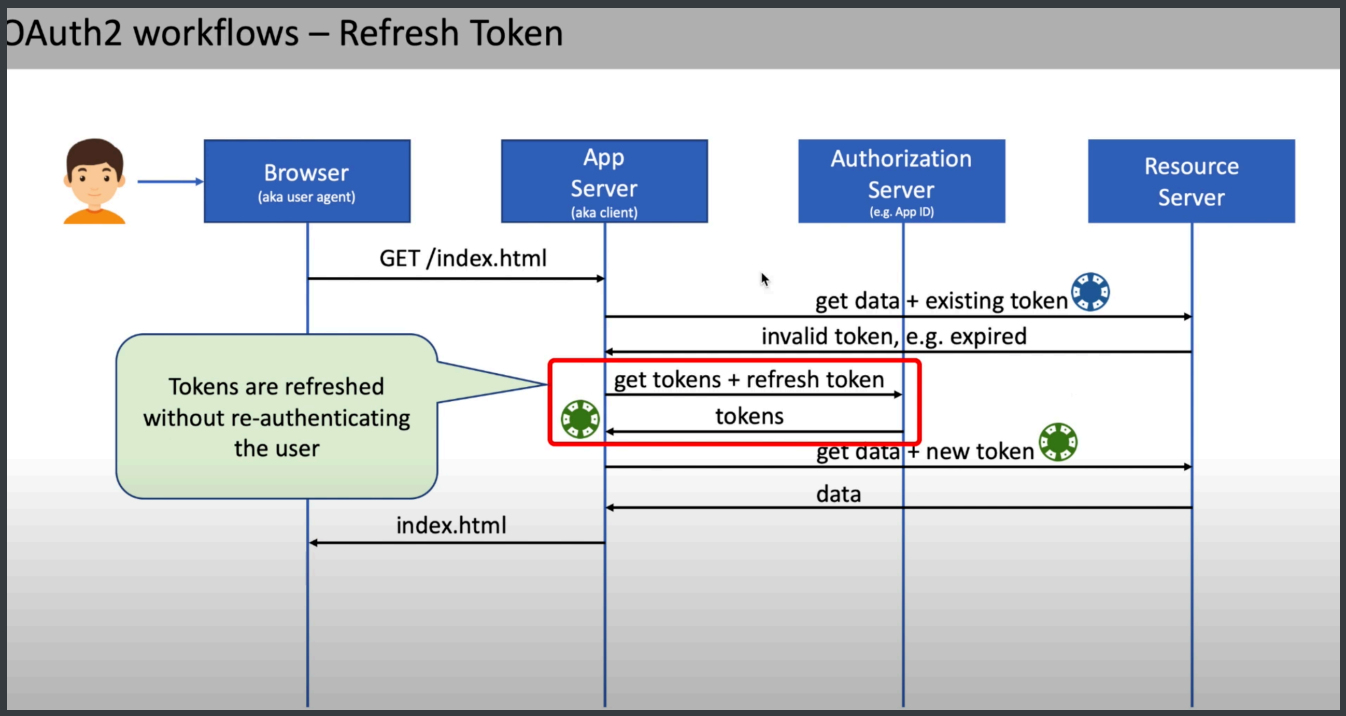
1. Authorization Server return the login form



2. App Server return the login form



3. Refresh token



ID token（based on OIDC「OpenID Connect」）

OpenID **a layer on top of OAuth2**

to verify user Identity

obtain profile information

ID token primary extension of OpenID

OAuth2 is an authorization framework

OIDC is an authentication layer on top of OAuth2

Access token represents authorization

ID token represents authentication (as JWT)

with **Access token** you want to know **What the user is authorized to do**

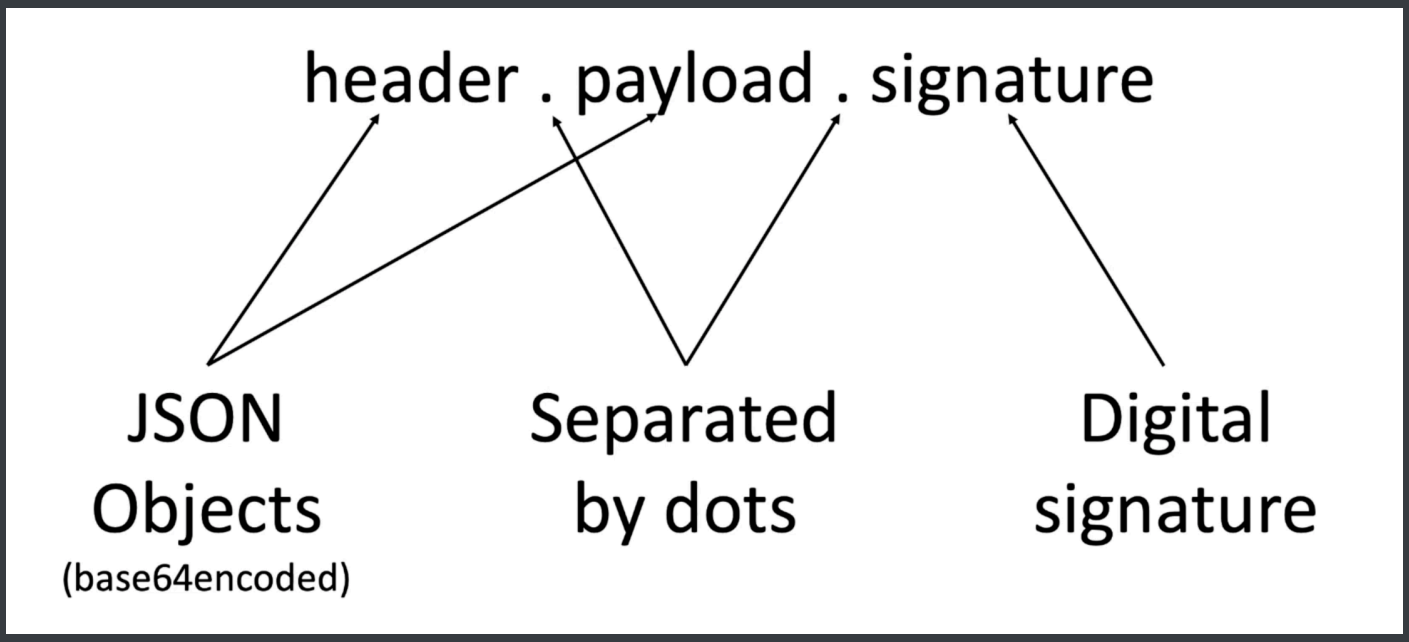
with **ID token** you want to know **who that user is**

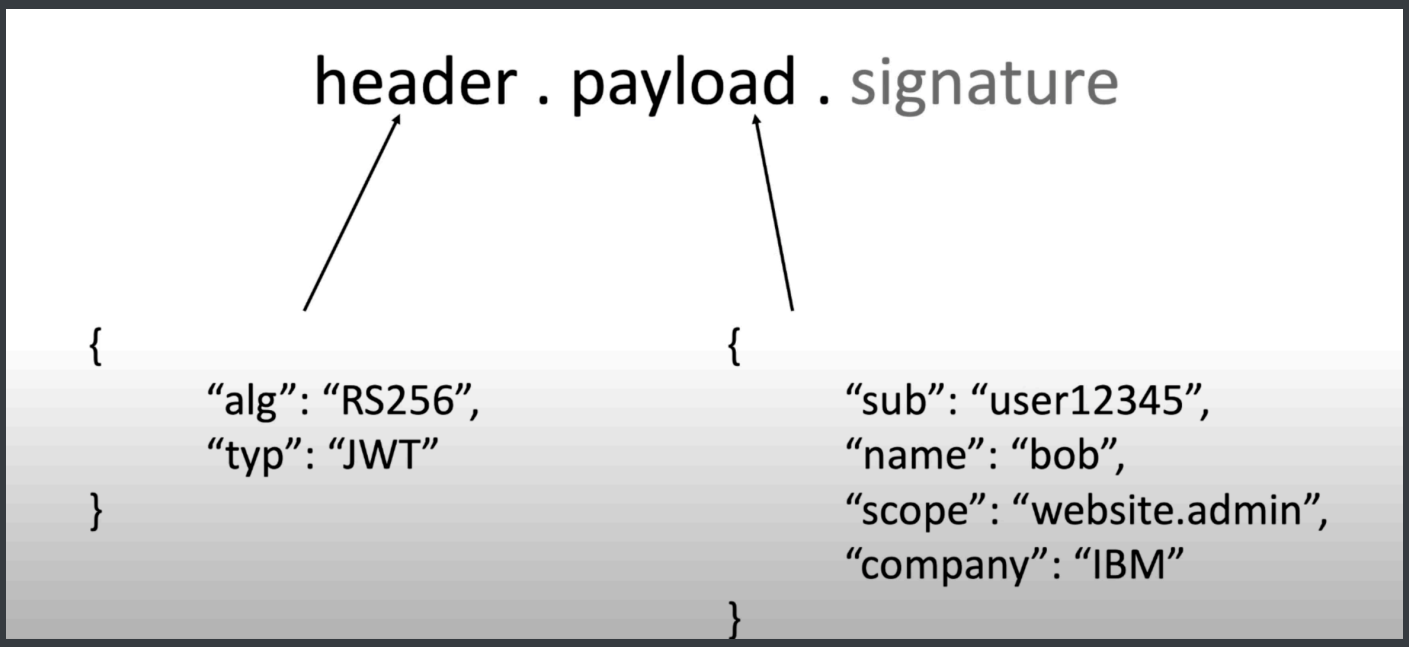
What is JSON Web Token (JWT)

JSON Web Token (aka JWT)

JWT is an open standard (RFC 7519) that defines a **compact** and self-contained way for **securely transmitting information** between parties as a **JSON object**. This information can be **verified and trusted** because it is **digitally signed**. JWTs can be signed using a secret (with the **HMAC** algorithm) or a public/private key pair using **RSA** or **ECDSA** (https://jwt.io/introduction)

Compact
Securely transmitting information
JSON object
Verified and trusted
Digitally signed





header . payload . signature

ewsJ4oCcYWxn4oCdOiDigJxSU0EyNTbigJ0sCgnigJx0eXDigJ06IOKAnEpXVOKAnQp9Cg ← Base64enoded header JSON object

.

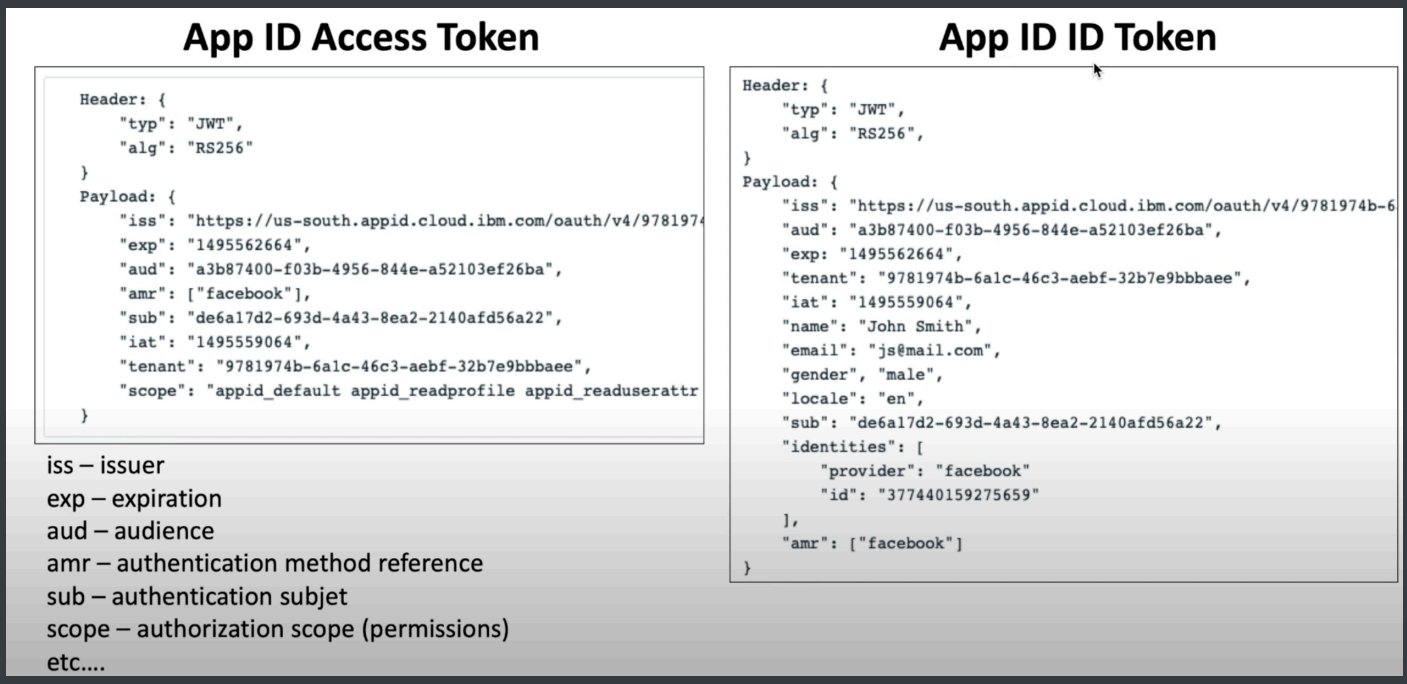
ewsJ4oCcc3Vi4oCdOiDigJx1c2VyMTIzNDXigJ0sCgnigJxuYW1l4oCdOiDigJxhbnRvbuKAnSwKCeKAnHNjb3Bl4oCdOiDigJx3ZWJzaXRlLmFkbWlu4oCdLAoJ4oCcY29tcGFueeKAnTog4oCcSUJN4oCdCQp9Cg ← Base64 encoded payload JSON object

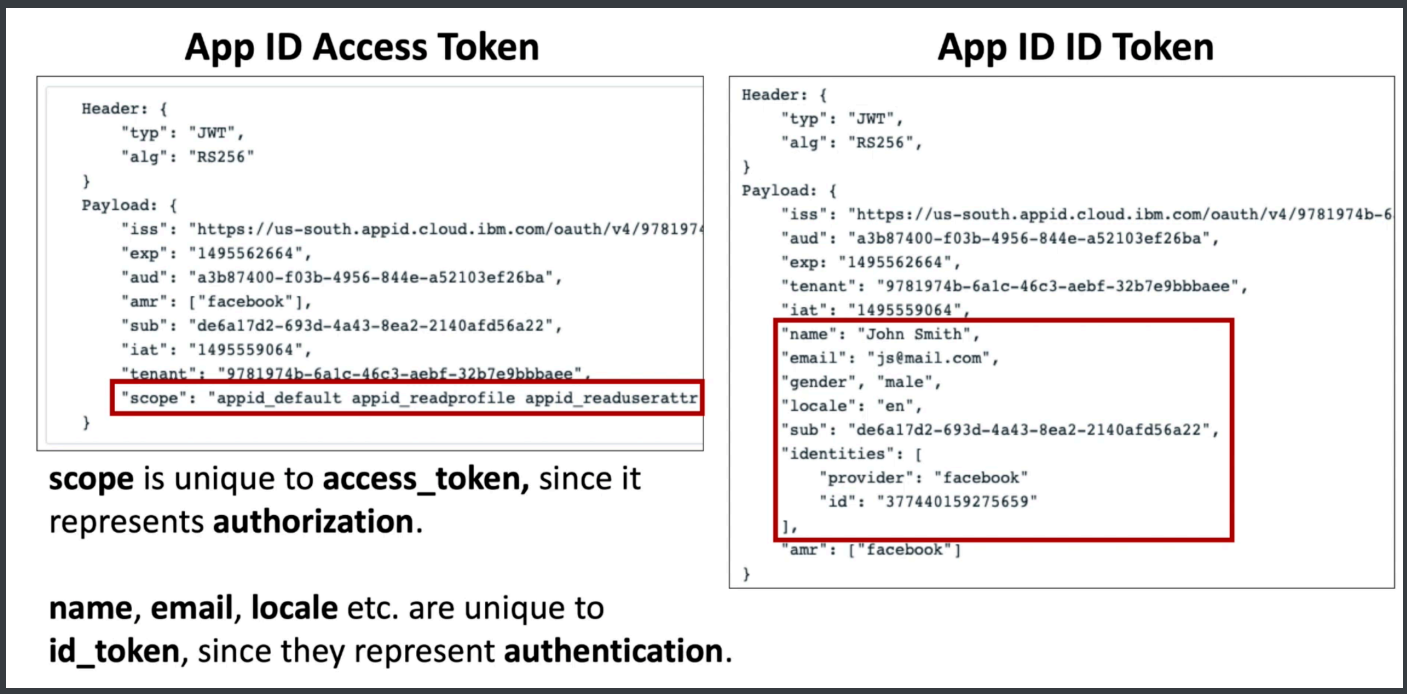
.

1l3tRGoXiYgO4O0/BjHNNwiAQF1q6q6nQ89SPKwA ← Digital signature

digital signature allows a receiving party to ensure that token is coming from authorized source

because tokens are signed using aprivate key and authorization servers are providing public key to validate token signatures, this way tokens are completly immutable





Bearer Token

Bearer Tokens are the predominant **type of access token** used with OAuth 2.0.

A Bearer Token is an opaque string, not intended to have any meaning to clients using it. Some servers will issue tokens that are a short string of hexadecimal characters, while others may use structured tokens such as JSON Web Tokens.
(https://oauth.net/2/bearer-tokens)

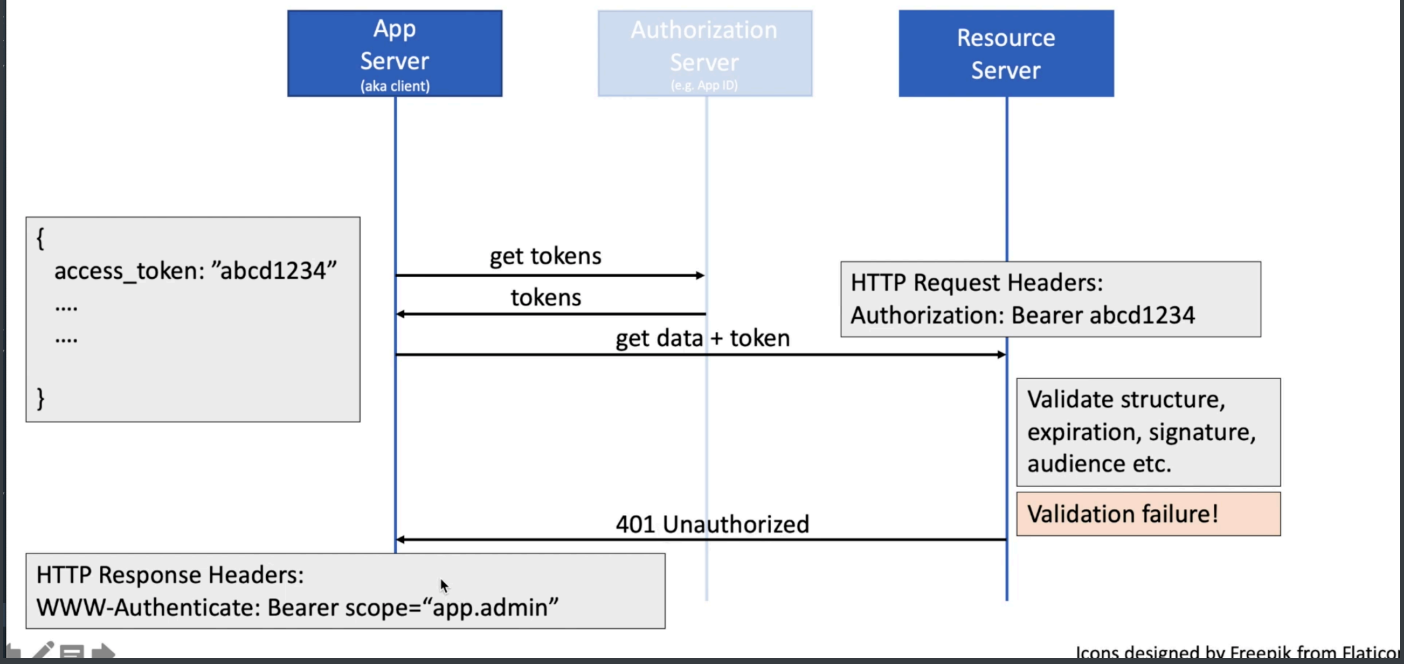
Type of access token

with particular rules how this token must be used to get access

it's a definition over protocol how to use access token

Bearer token means whoever bears the token can use it

Bearer Token workflow



Icons designed by Freepik from Flaticon

Summary

- **OAuth2** – Authorization framework
- **OpenID Connect** – Authentication framework on top of OAuth2
- **JSON Web Tokens** – Structured and secured way to store and transport information
- **Bearer Token** – type of access_token with a well-defined transport, validation, and access control behavior

Summary