Session 2:
Zero Trust API Access based on OAuth

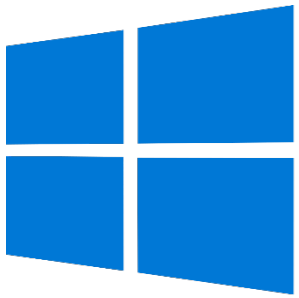
James Lee | Security Solutions Architect | F5

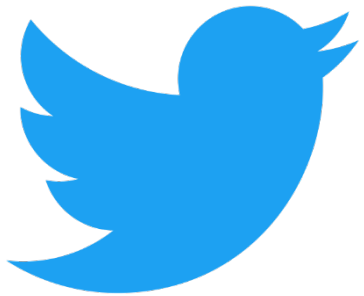
OAuth 2.0

What is OAuth 2.0?

AN OPEN STANDARD FOR AUTHORIZATION

- OAuth 2.0 is a delegation protocol.
- It allows a user to authorize access to a resource without sharing their credentials.
- The user who owns a resource can allow a 3rd party application to access the user's resource on their behalf in the OAuth framework.
- It is the most widely supported authorization/authentication(with OIDC extension) framework.







Types of API

User-to-App API Access

External APIs

- Authorized clients connecting from external.
- Responsefiles indicates the API calls from internal apps to external 3rd party APIs.

App-to-App API Access

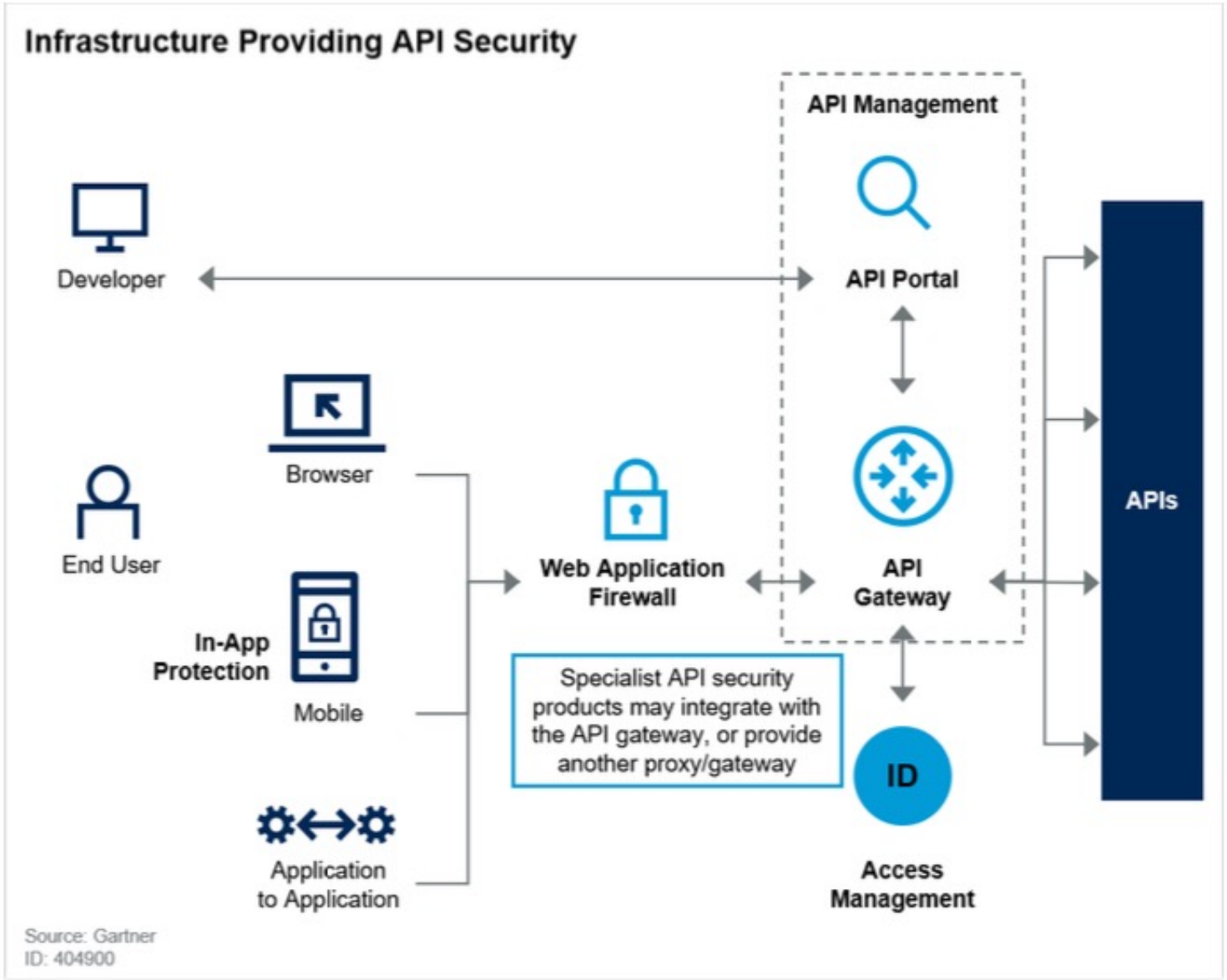
Partner APIs

- Available to selected and authorized external developers or API consumers.

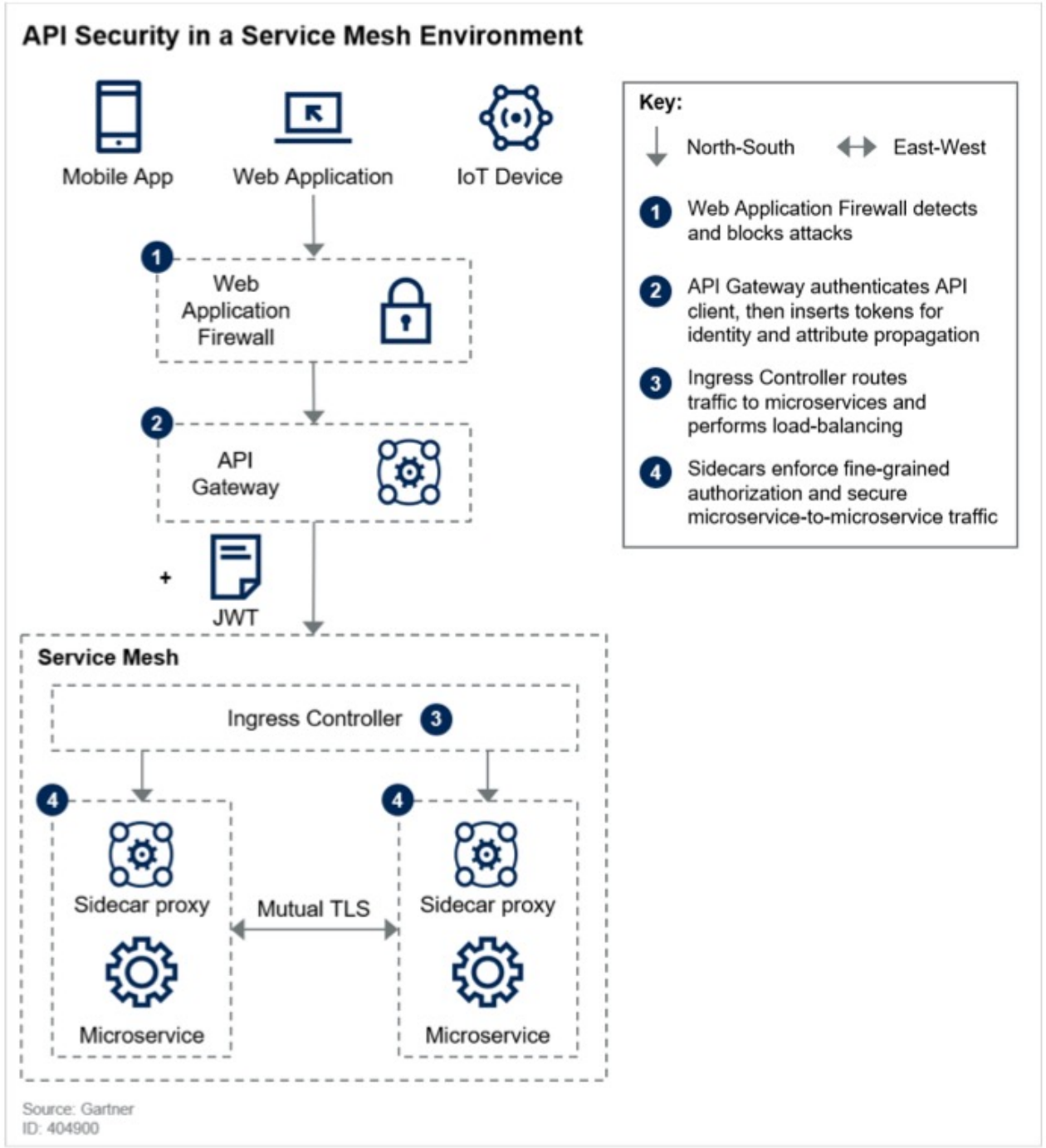
Internal APIs

- Use within the enterprise to connect systems and data within the business.
- Normally, it represents the App-to-App API calls or API calls from developers.

Layered Defense for API Security - Gartner

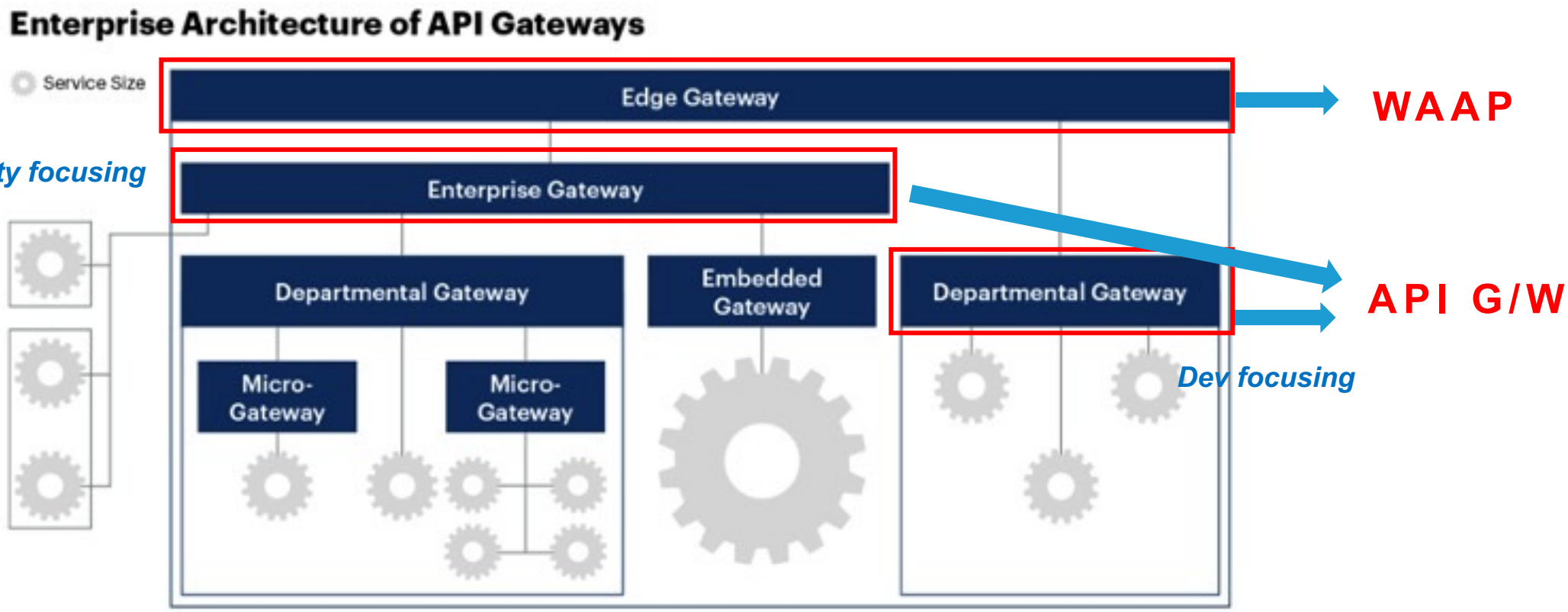


Zero Trust for User-to-App API Security



Gartner's API G/W design Architecture

Figure 3: Enterprise Architecture of API Gateways



Gartner

Two-tier API G/W Design

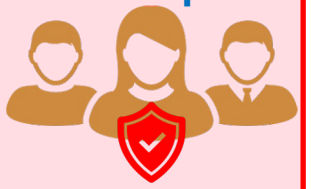
Coarse-grained API Access Control

- *Eliminate the weak cryptography algorithm*
- *Authenticate the user and enforce basic control. (e.g. Control HTTP methods based on group info. / Deny access to the admin API endpoints from external groups.)*
- *Enable mTLS as an additional authentication methods for partners.*
- *Blacklist for suspicious JWT list.*
- *Enforce OpenAPI spec.*

Browser App

Enterprise API G/W

SecOps



Coarse-grained Access Control

Departmental API G/W

API Owners (Dev Team)

Fine-grained Access Control

Fine-grained API Access Control

- *Enforce the object ID comparison for the specific API endpoints. (Preventing BOLA)*
- *Checking detailed user's privileges and enforcing the micro control.*
- *API-specific control policy can be enforced. (e.g. Max file-size limit for the file-uploading API endpoint.)*

{ api }

Zero Trust API Security Demo for User-to-App API Access

Secure Token Translation

Opaque Token (By-reference Token)

- Opaque Token doesn't contain any information about the grant
- The Client or Resource Server has to ask the Authorization Server every time it wants to know the validity or scope data for an Access Token
- This allows tokens to be revoked before they expire

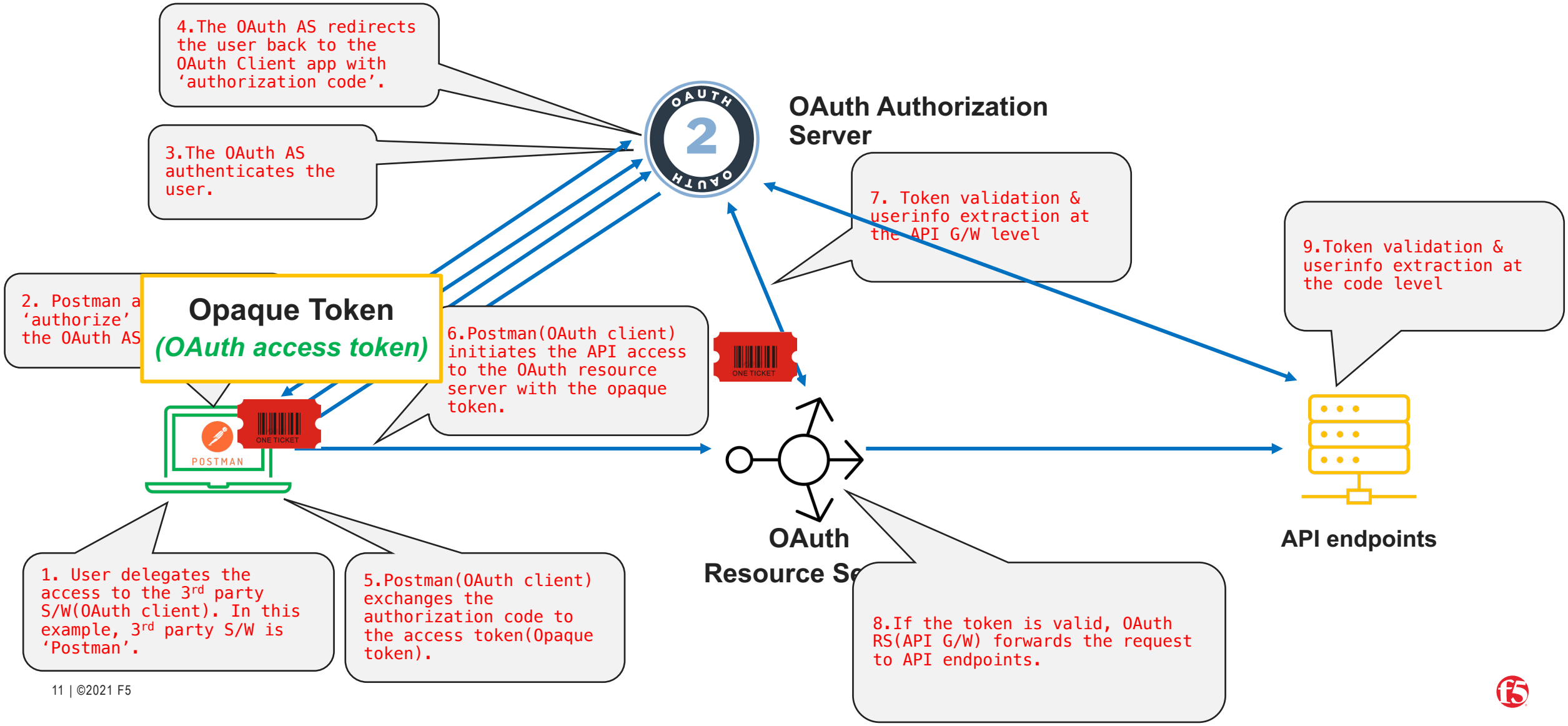
```
HTTP/1.1 200 OK
 Content-Type:
application/json;charset=UTF-8
 Cache-Control: no-store
 Pragma: no-cache

{

"access_token":"2YotnFZFEjr1zCsicMWpAA",
    "token_type":“bearer",
    “expires_in":3600,

"refresh_token":"tGzv3JOkF0XG5Qx2TlKWIA",
}
```

OAuth Token Flow – Opaque token



JWT Token (By-Value Token)

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c
```

Decoded EDIT THE PAYLOAD AND SECRET

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

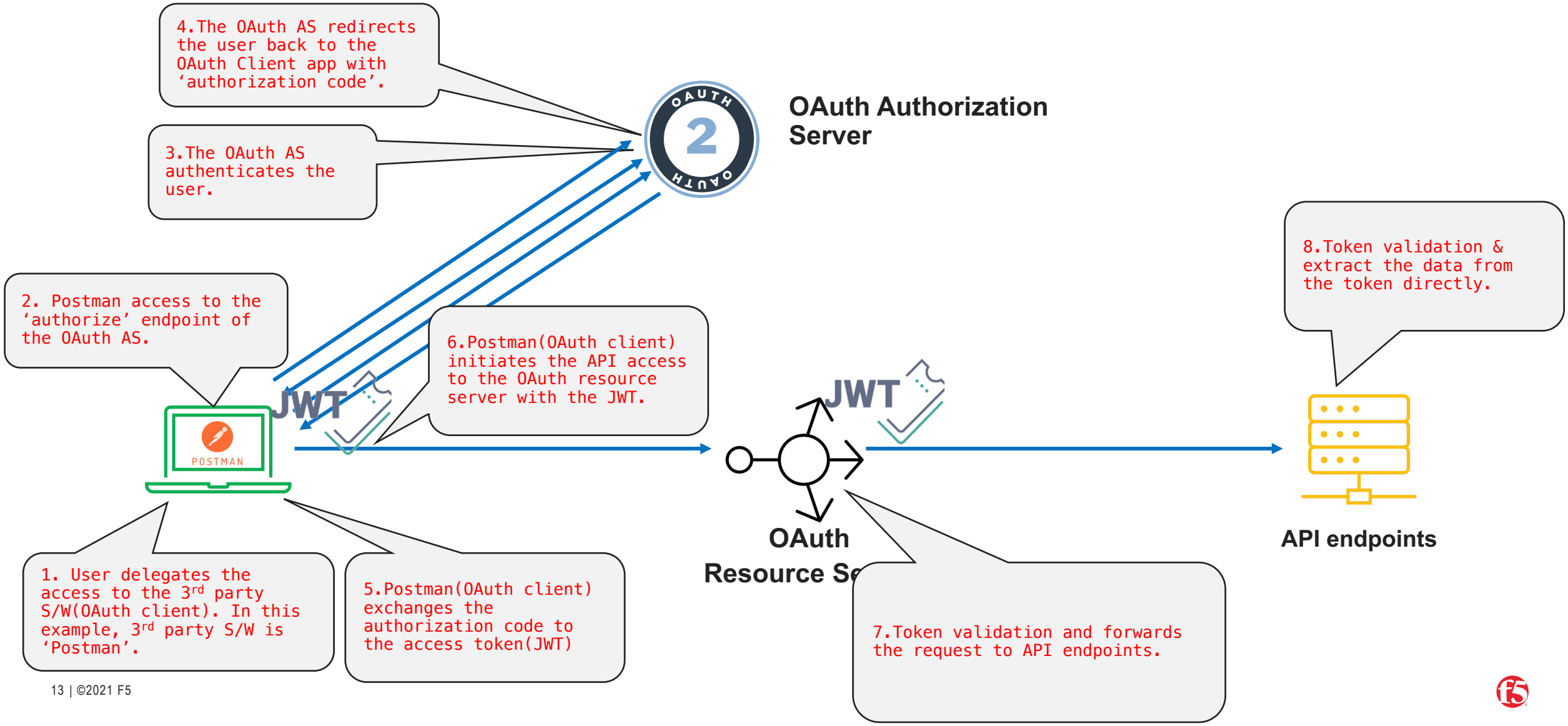
PAYLOAD: DATA

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
) ☐ secret base64 encoded
```

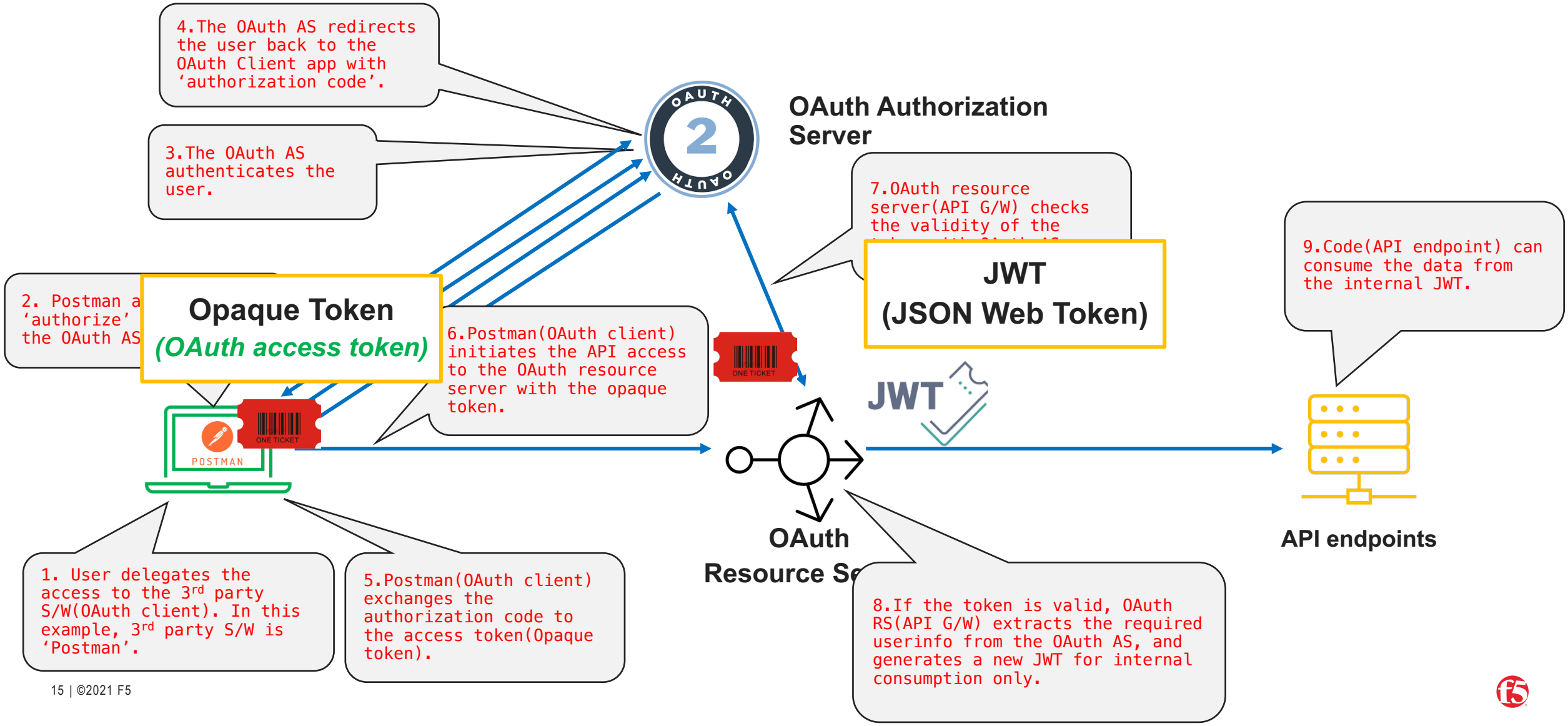
OAuth Token Flow – JWT



Opaque Token VS Transparent Token

Opaque Token	Transparent Token (JWT Token)
• Also called as ‘By-Reference’ token. • Randomly generated identifier. • Proprietary format. • Require validation from an ‘authorization server’. • Can be revoked. • Does not contain any real user data.	• Also called as ‘By-Value’ token. • It contains real user data. • Anyone can inspect the content. • Self-validation.
More secure but less scalable. Aligned with Zero trust Concept *[Never trust, Always verify]*	More scalable, faster but less secure.

Secure Token Translation – Normal Flow



Secure Token Translation – Token revocation