JWT

What is JWT?

JWT stands for Json Web Token is an internet standard used to secure json data that shared between client and server.

The structure of JWT:

Json web Token has three parts header(x), payload(y) and signature(z), and separated by dots.

Example: xxxxx.yyyyy.zzzzz

Header:

In this section there are two parts:

- Type of the token: JWT.
- Signing algorithm: SHA256, RSA or HMAC.

Example:

{

“alg” : ”HS256”,
“typ” : ”JWT”

}

then the head is Base64url encoded.

Payload:

This is the second section and it has claims, there are three types of claims registered, public, private.

Claims: are about entity (user).

Registered claims: are predefined and these some of claims issuer(iss), subject(sub),audience(aud), expiration time(exp) and others.

Public claims: are not registered with JWT specification, but it registered in IANA(Internet Assigned Number Authority), common public claims: name, email, nickname and more.

Private claims: these claims are similar to public but more details for example information about user’s department, role, organization and permissions.

Example for payload:

```
{
 “name”:”Ali”,
“email”:”ali@email.com”
}
```

then the payload is base64Url encoded.

Signature:

Combine header, payload and a secret, the algorithm specified in the header and sign that.

references

1- https://jwt.io/introduction
2- https://blog.postman.com/what-is-jwt/
3- https://kinde.com/guides/authentication/types-and-methods/json-web-token-claims/
4- https://developer.okta.com/blog/2020/12/21/beginners-guide-to-jwt#jwt-header