AccessToken Vs ID Token Vs Refresh Token - What? Why?When?

-
-

About JSON Web Tokens (JWT)

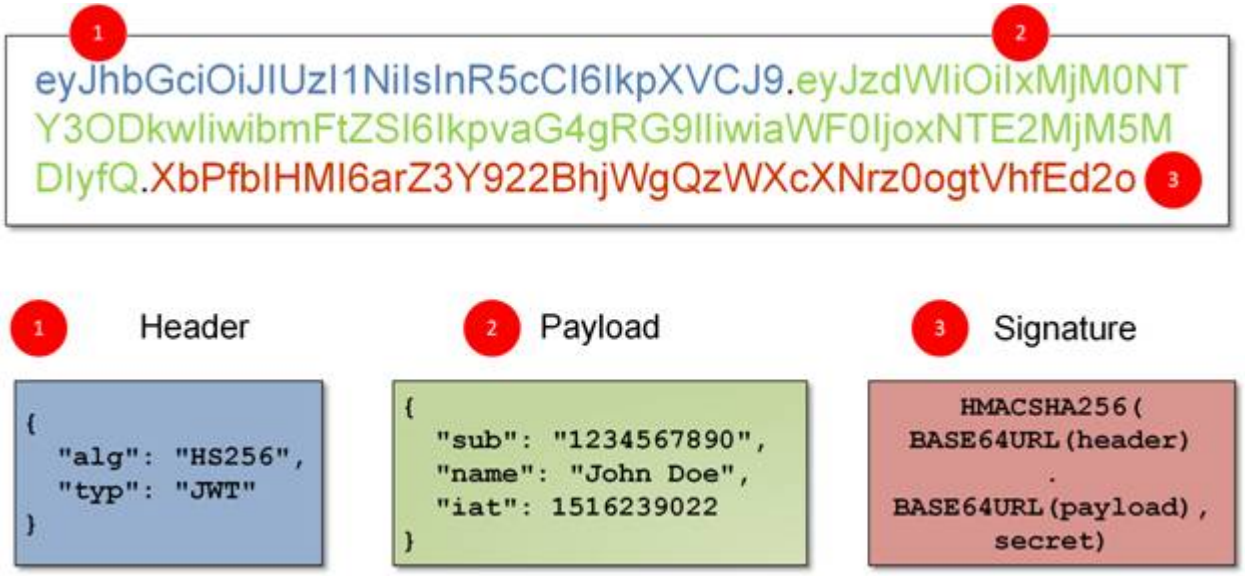
JWT i.e. Json Web Tokens, are an important piece in ensuring trust and security in your application. JWT allows claims such as user data to be represented in a secure manner.

A JWT is represented as a sequence of base64url encoded values that are separated by dot character. It's ideal format is like “Header.Payload.Signature”, where header keeps metadata for the token. The payload is basically the claims of the entity (typically user) and a signature for the signed token.

The Signed token is generated by combining the encoded JWT header and Payload and it is signed by using encryption algorithm like HMAC SHA–256. The signature private key is always held by server so it will be able to verify existing token as well as sign new token.

JWT could be used as an opaque identifier and could be inspected for additional information – such as identity attributes which it represents as claims.

Sample JWT token format could look like,



What is Access Token?

Access tokens are credentials used to access protected resources.

Access tokens are used as bearer tokens. A bearer token means that the bearer (who holds the access token) can access authorized resources without further identification.

Because of this, it is important that bearer tokens be protected.

These tokens usually have a short lifespan for security purpose. When it expires, the user must authenticate again to get a new access token limiting the exposure of the fact that it is a bearer token.

Access token must never be used for authentication. Access tokens cannot tell if the user has authenticated. The only user information the access token processes is the user id, located in sub claims.

The application receives an access token after a user successfully authenticates and authorizes access. Itis usually in JWT format but do not have to be.

The aplication should treat access tokens as opaque strings since they are meant for APIs. Your application should not attempt to decode them or expect receive token in a
particular format.

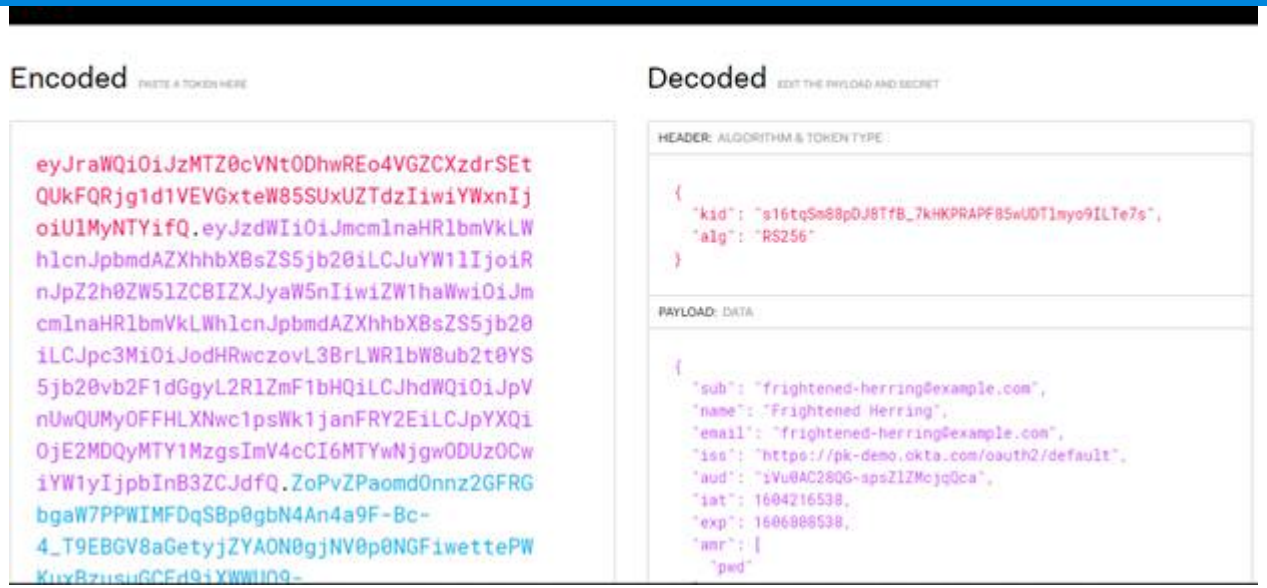
This token does not contain any information about the user itself besides theirs ID (“sub”).It only contains authorization information about which actions the application is allowed to perform at the API (“scope”). This is what makes it useful for securing an API, but not for authenticating a user.

An access token is put in the Authorization header of your request, usually looks like Bearer “access_token” that the API you are calling can verify and grant you access.

Example of Access Token

Here is the sample response from the token endpoint! The response includes the ID token and access token. Your application can use the access token to make API requests on behalf of the user.

```
{
  "token_type": "Bearer",
  "expires_in": 86400,
"access_token": "vCwWSQiaYhMHN2IbnEijtDWJ-BpiHbPohI6tOVrkrUrL2MqlF05K84MhBzvoC6iShEdUXl7t",
  "scope": "openid profile email photo",
  "id_token": "eyJraWQiOiJzMTZ0cVNtODhwREo4VGZCXzdrSEtQUkFQRjg1d1VEVGxteW85SUxUZTdzIiwiYWxnIjoiUlMyNT
Bc-4_T9EBGV8aGetyjZYAON0gjNV0p0NGFiwettePWKuxBzusuGCEd9iXWWUO9-
WTF5e2AGr3_jkg34dbxfiFXy3KgH7m0czm809cMaiZ_ofLYgJHVD8lqMQoWifhoNhpjPqa19Svc3nCHzSYHUgTXQWvA56NmQvyVPh
bOd7FL39jeam2-
k1TFSDogyJE513aC0OssRADr_TWvtL8xoaPkXM_7bXYs9_7erXmzF9la0hvmOuasieetpLhOvFeoiOJWCU9xhxj4Q"
}
```



Why do we need Access Token?

Access tokens are used to inform an API that the bearer of the token has been authorized to access the API and perform a predetermined set of actions specified by the scope. It is used to authorize API access.

What is ID Token?

OpenID Connect always issues ID token along with access token to provide compatibility with OAuthand match the general tendency for authorizing identity.

ID token carries personal information about end-users that authenticate on an OpenID Connect flow. In addition, this security token contains claims data about the user as saved with the authentication server.

The ID token represents as JWT.

For example, if there is an app that uses google to login in users and to sync their calendars, google sends Id token to the a that includes information about the user

means thata specific application should consume the token.

Identity token payload contains “auth_time” (when the end user actually authenticated), “iss” (who has issued the token), “aud” (Intended audience), “sub” (unique identifier of the user), “idp” etc.

Example of ID Token (JWT)

Here is the sample response from the token endpoint! The response includes the ID token and access token.

```
{
  "token_type": "Bearer",
  "expires_in": 86400,
  "access_token": "vCwWSQiaYhMHN2IbnEijtDWJ-BpiHbPohI6tOVrkrUrL2MqlF05K84MhBzvoC6iShEdUXl7t",
  "scope": "openid profile email photo",
"id_token": "eyJraWQiOiJzMTZ0cVNtODhwREo4VGZCXzdrSEtQUkFQRjg1d1VEVGxteW85SUxUZTdzIiwiYWxnIjoiUlMyNTYi
Bc-4_T9EBGV8aGetyjZYAON0gjNV0p0NGFiwettePWKuxBzusuGCEd9iXWWUO9-
WTF5e2AGr3_jkg34dbxfiFXy3KgH7m0czm809cMaiZ_ofLYgJHVD8lqMQoWifhoNhpjPqa19Svc3nCHzSYHUgTXQWvA56NmQvyVPh
bOd7FL39jeam2-
k1TFSDogyJE513aC0OssRADr_TWvtL8xoaPkXM_7bXYs9_7erXmzF9la0hvmOuasieetpLhOvFeoiOJWCU9xhxj4Q"
}
```

Why we need ID Token?

The ID token used to retrieve user’s basic profile informationlike name, DOB, email, phone, which is present in authentication server. ID token should not be used to gain access to an API.

What is Refresh token?

- This token is a long-lived token compared to the access token and is used to request a new access token in cases where it is expired.
- It can be considered as credentials used to obtain access tokens.
- It's allowed for long-lived access and highly confidential.

- You will receive this in an encoded format only that cannot be decoded. An example could be 494c427ace9e04dea03c7234cea96c5ca53e0ce4ea95147e961fd9ebcf8feb84

Example of Refresh Token

Here is the sample response from the token endpoint! The response includes the access token along with the refresh token.

```
{
  "access_token":"ya29.a0AfH6SMARVjPq6G2y_P3hn3mbDdnRVrTGwO1ZkTXvUHye9wcpAPyiRKilq6Wh20TRbVx0nA1Nn8z1
NWwuckHpiaOfr_uITriM0aS2t3HbGIKQJiU",
  "scope":"https://mail.google.com/",
  "token_type":"Bearer",
  "expires_in":3599,
  "refresh_token":"1//0419Pth1mYFyBCgYIARAAGAQSNwF-L9IrcV8zK4wHDznJqUbeXrcEoE2O-
Tmz7ryNpztTrLOiYOvs-0z4hxddGBpcKc0pEzLcWFI"
}
```

Why do we need Refresh token?

As access token has defined lifetimes, and there could be a possibility that the current access token becomes invalid or expires. This is the token used to request new access tokens without user interaction.

Requesting an access token using a refresh token

While requesting a refresh token, scope should be set as offline_access to the scope parameter.

```
Method: POST
Content-Type: application/x-www.form-urlencoded
Authorization: Bearer “access token”
https://authorization-server.com/token?
grant_type=refresh_token
&refresh_token =<<refresh_token>>
&scope=offline_access
```

```
{
  "token_type": "Bearer",
  "expires_in": 86400,
  "access_token": "QKY08tqDO8aeNebZbfgUFs1PH-cjerK2WBvE9FZpYGgZHnS_nLfhKYTECMBmPF_chz5GipOA",
  "scope": "photo offline_access",
  "refresh_token": "8V2dMpzRqB5cQDvoTb6X_Msl"
}
```

Summary

Below is the quick reference of all the tokens at a glance,

- *Access token* used in token-based authentication to gain access to resources by using them as bearer tokens.
- *Refresh token* is a long-lived special kind of token used to obtain a renewed access token.
- *ID token* carries identity information encoded in the token itself, which must be a JWT. It must not contain any authorization information, or any audience information — it is merely an identifier for the user.