**Section10 Refresh Token**

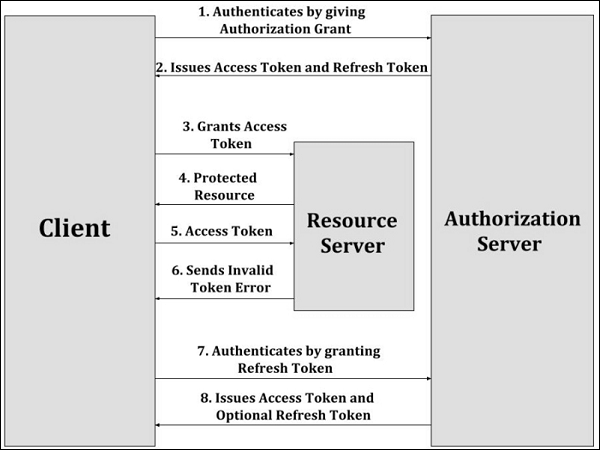
**Notes: -**

**1-Refresh tokens are the credentials that can be used to acquire new access tokens.**

**A-The lifetime of a refresh token is much longer compared to the lifetime of an access token.**

**B-Refresh tokens can also expire but are quiet long-lived.**

**C-When current access tokens expire or become invalid, the authorization server provides refresh tokens to the client to obtain new access token.**



**1-the client authenticates with the authorization server by giving the authorization grant.**

**2- the authorization server authenticates the client, validates the authorization grant and issues the access token and refresh token to the client, if valid.**

**3-Then, the client requests the resource server for protected resource by giving the access token.**

**4- The resource server validates the access token and provides the protected resource.**

**5- The client makes the protected resource request to the resource server by granting the access token, where the resource server validates it and serves the request, if valid. This step keeps on repeating until the access token expires.**

**6- If the access token expires, the client authenticates with the authorization server and requests for new access token by providing refresh token. If the access token is invalid, the resource server sends back the invalid token error response to the client.**

**7- The client authenticates with the authorization server by granting the refresh token.**

**8- The authorization server then validates the refresh token by authenticating the client and issues a new access token, if it is valid.**

**So with using refresh token the client communicate with the resource server to check if the token is valid or not with the resource server while the token is valid or not and if the token is invalid it will send authorized request to the authorization server to generate new token.**

**We see also that the resource server return response resources in secure way to protect and ensure that the sender is the same not anyone else.**

**1-on the normal way if you change the expire time for the token generated to 1 millisecond , the client will be take effect to 5 minutes**

**So you have to set the**

**config.TokenValidationParameters = new TokenValidationParameters(){**

**//it will make the client authentication expiration to zero so it will make the client**

**ClockSkew = TimeSpan.Zero,**

**ValidIssuer = JWTSettings.Issuer,**

**ValidAudience = JWTSettings.Audiance,**

**IssuerSigningKey = key,};**