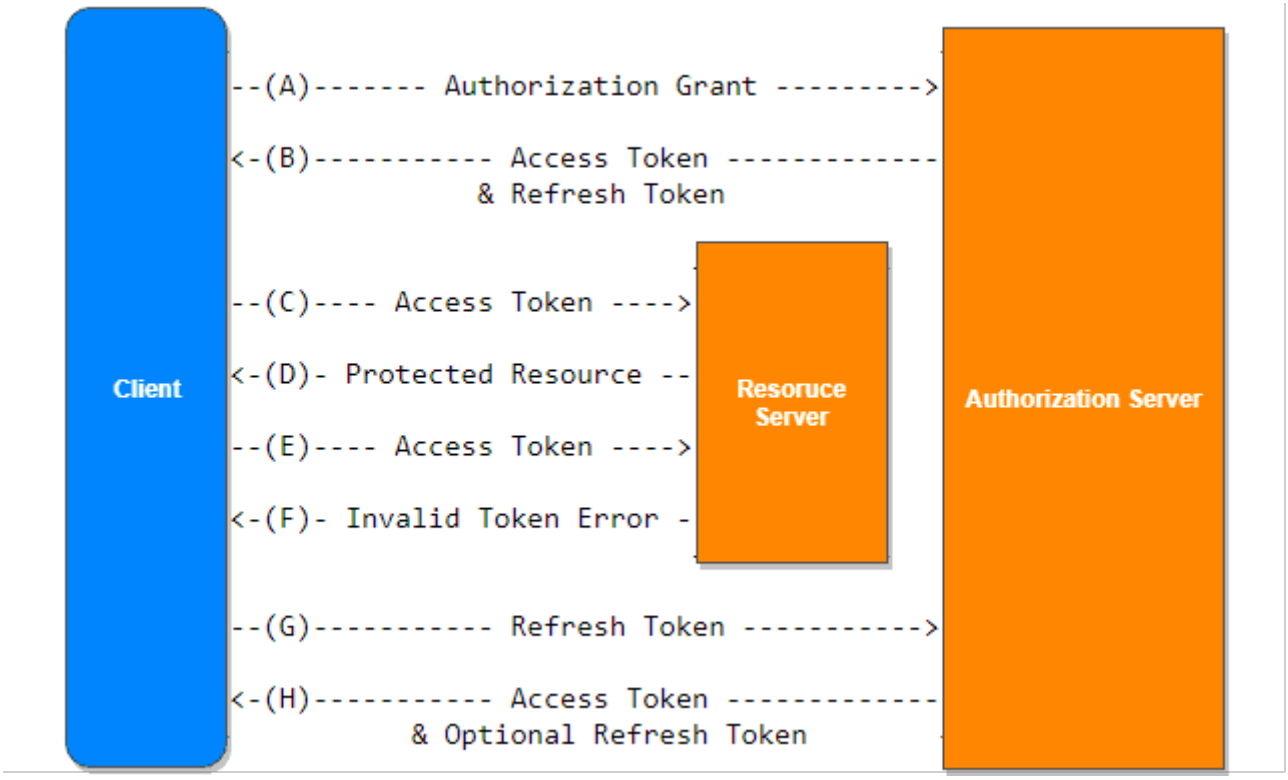
Refresh Token (Yenileme Token'ı)

Refresh token (yenileme token'ı), **access token**'ın süresi dolduğunda veya geçersiz hale geldiğinde yeni bir **access token** almak için kullanılan bir kimlik doğrulama aracıdır. Refresh token, istemciye **authorization server (yetkilendirme sunucusu)** tarafından verilir ve **resource server (kaynak sunucu)** ile doğrudan kullanılmaz. Refresh token, istemcinin sürekli olarak erişim sağlamak için yeni **access token**'lar alabilmesine imkan tanır.

Refresh Token'ın Temel Özellikleri:

1. **Yeni Access Token Alma:**
    - Refresh token, geçerli bir **access token**'ın süresi dolduğunda veya token geçersiz hale geldiğinde yeni bir access token almak için kullanılır. Access token'ın süresi genellikle kısa olur, bu yüzden refresh token ile yeni token almak gerekir.
2. **Sadece Yetkilendirme Sunucusunda Kullanım:**
    - Refresh token yalnızca **authorization server** ile etkileşime girmekte kullanılabilir. **Resource server** (kaynak sunucu) refresh token'ı almaz ve bu token herhangi bir şekilde bu sunuculara iletilmez.
3. **Genellikle Opak Yapı:**
    - Refresh token genellikle istemci için **opak** (şeffaf olmayan) bir dizedir. İstemci, token'ın içeriğini doğrudan göremez; ancak authorization server, bu token'ı doğrulayıp yeni bir access token sağlayabilir.
4. **Verilen Yetkiler:**
    - Refresh token, istemciye **resource owner (kaynak sahibi)** tarafından verilen yetkileri temsil eder ve bu token, access token ile aynı yetkileri taşıyan yeni token'ların alınmasına imkan tanır.
5. **Yeniden Kullanım:**
    - **Refresh token** yalnızca authorization server ile etkileşimde kullanılabilir. Bu token, **resource server** ile paylaşılmaz. Refresh token, genellikle uzun süre geçerli olabilir, ancak authorization server, ihtiyaç durumuna göre yeni bir refresh token verebilir.



Refresh Token (Yenileme Token'ı)

Refresh token (yenileme token'ı), **access token**'ın süresi dolduğunda veya geçersiz hale geldiğinde yeni bir **access token** almak için kullanılan bir kimlik doğrulama aracıdır. Refresh token, istemciye **authorization server (yetkilendirme sunucusu)** tarafından verilir ve **resource server (kaynak sunucu)** ile doğrudan kullanılmaz. Refresh token, istemcinin sürekli olarak erişim sağlamak için yeni **access token**'lar alabilmesine imkan tanır.

Refresh Token'ın Temel Özellikleri:

1. **Yeni Access Token Alma:**
    - Refresh token, geçerli bir **access token**'ın süresi dolduğunda veya token geçersiz hale geldiğinde yeni bir access token almak için kullanılır. Access token'ın süresi genellikle kısa olur, bu yüzden refresh token ile yeni token almak gerekir.
2. **Sadece Yetkilendirme Sunucusunda Kullanım:**
    - Refresh token yalnızca **authorization server** ile etkileşime girmekte kullanılabilir. **Resource server** (kaynak sunucu) refresh token'ı almaz ve bu token herhangi bir şekilde bu sunuculara iletilmez.
3. **Genellikle Opak Yapı:**
    - Refresh token genellikle istemci için **opak** (şeffaf olmayan) bir dizedir. İstemci, token'ın içeriğini doğrudan göremez; ancak authorization server, bu token'ı doğrulayıp yeni bir access token sağlayabilir.
4. **Verilen Yetkiler:**

- Refresh token, istemciye **resource owner (kaynak sahibi)** tarafından verilen yetkileri temsil eder ve bu token, access token ile aynı yetkileri taşıyan yeni token'ların alınmasına imkan tanır.

5. **Yeniden Kullanım:**
    - **Refresh token** yalnızca authorization server ile etkileşimde kullanılabilir. Bu token, **resource server** ile paylaşılmaz. Refresh token, genellikle uzun süre geçerli olabilir, ancak authorization server, ihtiyaç durumuna göre yeni bir refresh token verebilir.

Refresh Token Akışı (Şekil 2):

Refresh token'ın kullanımını anlamak için aşağıdaki akışa göz atalım:

1. **Adım A:**
    - **Client (İstemci)**, authorization server'a bir **authorization grant** ile başvurarak bir access token talep eder.
2. **Adım B:**
    - Authorization server, istemciyi kimlik doğrulaması yaparak ve authorization grant'ı doğrulayarak bir **access token** ve **refresh token** verir.
3. **Adım C:**
    - İstemci, access token'ı kullanarak **resource server**'a korunan kaynağa erişim talep eder.
4. **Adım D:**
    - **Resource server** access token'ı doğrular ve geçerliyse kaynakla ilgili işlemi gerçekleştirir.
5. **Adım E:**
    - Adım C ve D tekrarlanır. Access token'ın süresi dolana kadar bu adımlar devam eder.
6. **Adım F:**
    - Access token süresi dolmuşsa, **resource server** geçersiz token hatası döndürür.
7. **Adım G:**
    - İstemci, **refresh token**'ı kullanarak authorization server'a başvurarak yeni bir access token talep eder.
8. **Adım H:**
    - Authorization server, refresh token'ı doğrular ve geçerliyse yeni bir access token (ve isteğe bağlı olarak yeni bir refresh token) verir.

Refresh Token ile Erişim Token'ı Yenileme Süreci:

- **Step (A) to (B):** İstemci bir authorization grant ile **access token** ve **refresh token** almak için authorization server'a başvurur.
- **Step (C) to (D):** İstemci, **access token**'ı kullanarak protected resource'a erişim talep eder. **Resource server**, token'ı doğrular ve geçerli ise erişim izni verir.

- **Step (E) to (F): Access token** süresi dolarsa, resource server geçersiz token hatası verir.
- **Step (G) to (H):** İstemci, **refresh token** ile yeni bir **access token** alır.

Refresh Token’ın Avantajları:

1. **Sürekli Erişim:**
    - Refresh token, istemcinin kesintisiz bir şekilde kaynaklara erişmesini sağlar. Bir kere kullanıldığında istemci, sürekli olarak yeni access token'lar alarak kaynağa erişebilir.
2. **Token Yönetimini Kolaylaştırma:**
    - Access token'ların geçerlilik sürelerinin kısa tutulması güvenliği artırır, ancak refresh token kullanılarak istemci sürekli olarak yeni token alabilir. Bu, güvenliği sağlamanın yanı sıra token yönetimini daha verimli hale getirir.
3. **İleri Düzey Güvenlik:**
    - **Access token**'ların kısa süreli geçerliliği, potansiyel kötüye kullanım durumlarında riskleri azaltır. **Refresh token** yalnızca authorization server ile kullanıldığından, istemci ve resource server arasındaki güvenlik seviyesi artırılır.

Refresh Token Kullanımı ve Güvenlik:

- Refresh token'lar güvenli bir şekilde saklanmalıdır, çünkü **resource server** ile hiç paylaşılmazlar ve bu token'lar ile yeni **access token** alınabilir.
- **Authorization server** güvenlik politikalarına göre refresh token'ın süresini ve geçerliliğini yönetebilir. Örneğin, bir **refresh token** yalnızca belirli bir süre sonra geçerliliğini yitirebilir.

Sonuç:

Refresh token, OAuth 2.0 protokolünde istemcilerin **access token**'larının süresi dolduğunda veya geçersiz hale geldiğinde yeni bir token almak için kullandığı önemli bir araçtır. Bu token, **authorization server** ile etkileşimde bulunarak yeni **access token**'lar alınmasına olanak tanır ve sürekli bir erişim sağlar. Refresh token'ın yalnızca **authorization server** ile kullanılması, güvenlik açısından önemli bir avantaj sunar.