6. Refreshing an Access Token

Bu bölüm, bir istemcinin mevcut bir erişim belirtecinin süresi dolduğunda veya yenilenmesi gerektiğinde, **refresh token** kullanarak yeni bir erişim belirteci talep etme sürecini açıklamaktadır.

Yenileme Talebi (Refresh Request)

İstemci, yeni bir erişim belirteci almak için bir **refresh token** kullanır ve aşağıdaki parametreleri içeren bir HTTP isteği yapar. İstek, `application/x-www-form-urlencoded` formatında ve **UTF-8** karakter kodlamasıyla gönderilir.

Talep Parametreleri

1. **grant_type (Zorunlu):**
    - Değeri **"refresh_token"** olarak ayarlanmalıdır.
    - Bu, talebin bir yenileme talebi olduğunu belirtir.
2. **refresh_token (Zorunlu):**
    - Daha önce istemciye verilen refresh token.
    - Bu, yeni bir erişim belirteci almak için kullanılır.
3. **scope (Opsiyonel):**
    - Talep edilen erişim kapsamı (isteğe bağlıdır).
    - Kaynak sahibinin başlangıçta verdiği kapsam dışında bir kapsam talep edilemez.
    - Eğer belirtilmezse, başlangıçta verilen kapsam varsayılan olarak kullanılır.

Refresh Token Güvenliği

- **Refresh token**, uzun süre geçerli olan bir kimlik bilgisi olduğu için, yalnızca token'ı alan istemciyle bağlantılıdır.
- İstemci tipi "confidential" ise veya istemciye kimlik doğrulama bilgileri verildiyse (örneğin istemci kimlik bilgileri), istemci yetkilendirme sunucusuyla kimlik doğrulaması yapmalıdır.

Örnek HTTP Yenileme Talebi

Aşağıda, bir istemcinin güvenli bir bağlantı üzerinden yaptığı örnek yenileme talebi verilmiştir:

```
POST /token HTTP/1.1
Host: server.example.com
Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
Content-Type: application/x-www-form-urlencoded

grant_type=refresh_token&refresh_token=tGzv3JOkF0XG5Qx2TlKWIA
```

Detaylar:

- **Authorization Header:**
    - İstemci kimlik doğrulama bilgilerini içerir (örneğin, Base64 ile kodlanmış istemci kimliği ve istemci sırrı).
- **grant_type ve refresh_token:** Talebin içeriğinde gönderilir.

Yetkilendirme Sunucusunun Sorumlulukları

Yetkilendirme sunucusu, yenileme talebi sırasında aşağıdaki adımları takip etmelidir:

1. **İstemci Kimlik Doğrulaması:**
    - Confidential istemciler ve kimlik bilgileri verilen istemciler için kimlik doğrulama yapılmalıdır.
    - Refresh token'ın doğrulanan istemciye ait olduğundan emin olunmalıdır.
2. **Refresh Token Doğrulaması:**
    - Sağlanan refresh token geçerli ve yetkilendirilmiş olmalıdır.
3. **Erişim Belirtecini Yenileme:**
    - Eğer talep geçerliyse, istemciye yeni bir erişim belirteci verilmelidir.

Yeni Refresh Token Verme Seçeneği

- Yetkilendirme sunucusu, istemciye yeni bir refresh token sağlayabilir.
    - **Yeni refresh token verilirse:** İstemci eski refresh token'ı iptal etmeli ve yeni token'ı kullanmalıdır.
    - **Eski refresh token iptali:** Yeni bir refresh token sağlanırsa, sunucu eski refresh token'ı iptal edebilir.
- **Yeni Token'ın Kapsamı:**
    - Yeni refresh token verilirse, istemci tarafından sağlanan refresh token'ın kapsamı ile aynı olmalıdır.

Hata Durumları

Eğer:

- Talep doğrulama başarısız olursa,
- Refresh token geçersizse,
- İstemci kimlik doğrulaması yapılamazsa, **yetkilendirme sunucusu**, bir hata yanıtı döner .

Özet

Refresh token, istemcinin kaynak sahibinin yeniden müdahalesine gerek kalmadan yeni bir erişim belirteci talep etmesini sağlar. Bu süreç, güvenlik açısından dikkatle yönetilmeli, istemci kimlik

doğrulaması ve refresh token doğrulaması kesinlikle yapılmalıdır. Sunucu, refresh token'ın yanlış kullanılmasını önlemek için belirli durumlarda yeni bir refresh token verme ve eski token'ı iptal etme mekanizması sağlayabilir.