Access Token (Erişim Token'ı)

Access token, korunan kaynaklara erişim sağlamak için kullanılan bir kimlik doğrulama aracıdır. Bu token, istemcinin kaynaklara erişim hakkını temsil eden bir dizedir ve genellikle istemci tarafından şeffaf bir biçimde kullanılır. Access token, kaynak sahibi tarafından istemciye verilen yetkilere dayalı olarak belirli **kapsamlar (scope)** ve **erişim süreleri** içerir. Bu bilgiler, **resource server (kaynak sunucu)** ve **authorization server (yetkilendirme sunucu)** tarafından denetlenir.

Erişim Token'ının Temel Özellikleri:

1. **Kimlik Doğrulama Aracı:**
    - Access token, bir istemcinin kaynaklara erişim hakkını temsil eder. Bu, istemcinin, belirli bir **kapsama** ve **süreye** sahip olarak kaynaklara erişmesini sağlar.
2. **Opaklık (Opaque) Yapı:**
    - Token, genellikle istemci için **opak** yani şeffaf olmayan bir yapıdadır. Bu, istemcinin token'ın içeriğini anlamadığı, ancak bu token'ın geçerliliğini **resource server**'a sunarak erişim alabileceği anlamına gelir.
    - Bununla birlikte, bazı token'lar **kendisi içinde kimlik doğrulama bilgilerini** barındırabilir ve doğrulama yapıldığında bu bilgiler **verifiye** edilebilir.
3. **Kapsamlar ve Süreler:**
    - Erişim token'ları, **kaynak sahibi tarafından verilen yetkiler** doğrultusunda **belirli bir erişim kapsamı** ve **geçerlilik süresi** içerir. Örneğin, bir token yalnızca fotoğraf yüklemek için geçerli olabilir, başka bir token ise fotoğraf okuma yetkisi verebilir.
    - Token'ın geçerlilik süresi sona erdiğinde, istemcinin yeniden yetkilendirilmesi veya yenilenen bir token alması gerekebilir.
4. **Token Formatı:**
    - **Access token**'ların formatları farklılık gösterebilir. Bazı token'lar yalnızca bir kimlik (identifier) taşıyabilir, bazen ise **veri ve imza** içerebilir. Bu tür token'lar genellikle **JWT (JSON Web Token)** gibi standartlarla ifade edilir ve içerikleri doğrulanabilir. Örneğin, bir JWT token'ı, verileri ve bir dijital imzayı içerebilir, bu da onu doğrulamak için kullanılan **public key**'in gerekliliğini ortaya koyar.
5. **Gizlilik ve Güvenlik:**
    - **Access token**'lar genellikle **gizlidir**. Token'ın içeriği, yalnızca ilgili **resource server** tarafından anlaşılır ve doğrulanabilir. Bu, istemcinin token'ı doğru şekilde kullanabilmesi için ek kimlik doğrulama bilgilerine sahip olabileceği anlamına gelir. Ancak bu bilgiler, bu spesifikasyonun kapsamı dışında kalmaktadır.
6. **Tekrar Kullanılabilirlik:**
    - **Access token** tek bir kullanım için verilir, yani istemci bu token'ı kullanarak korunan kaynağa bir erişim isteği gönderir ve **resource server**, token'ı doğrulayıp yetkilendirme kararını verir.

Erişim Token'ının Avantajları:

1. **Basitleştirilmiş Kimlik Doğrulama:**
    - **Erişim token'ları**, farklı kimlik doğrulama yöntemlerini (örneğin, kullanıcı adı ve şifre gibi) tek bir token ile değiştirebilir. Bu, **resource server**'ın, farklı kimlik doğrulama yöntemlerini anlamak zorunda olmadan, **token**'ı doğrulayıp erişimi yönetmesine olanak tanır.
2. **Kapsamlı Güvenlik Sağlar:**
    - **Access token**'lar, yalnızca belirli bir **kapsama** ve **süreye** dayanarak sınırlı erişim sağlar. Bu, istemcinin yalnızca yetkilendirildiği kaynaklara ve işlevlere erişmesini sağlar.
3. **Esneklik ve Çeşitli Kullanım Yöntemleri:**
    - Token'lar farklı **formatlar** ve **kriptografik yöntemler** kullanılarak yapılandırılabilir. Bu, **resource server**'ın güvenlik gereksinimlerine göre token'ların biçimini ve kullanımını esnek bir şekilde uyarlamasına olanak tanır.
4. **Kapsamlı Uygulama Alanı:**
    - Bu token, çeşitli **kaynak sunucuları** tarafından kabul edilebilir. Yani bir istemci, birden fazla kaynağa erişim talep edebilir ve her bir kaynak için geçerli olan bir token alabilir.

Token'ın Yapısı ve Kullanımı:

1. **Şeffaf Olmayan Token (Opaque Token):**
    - Bu tür token, istemciye ne içerdiği hakkında bilgi vermez. Token'ı yalnızca **resource server** doğrulayabilir. Bu tür token'lar genellikle güvenlik amacıyla tercih edilir.
2. **JSON Web Token (JWT) gibi Yapılar:**
    - Bazı durumlarda, token'lar **JWT** gibi standartlara dayanır. JWT, hem verileri hem de bir imzayı içerir ve bu imza sayesinde token doğrulama yapılabilir. Bu tür token'lar **self-contained** yani kendi kendine doğrulanabilir yapıdadır.

Özet:

Access token, OAuth 2.0 protokolünde istemcilerin, kaynaklara erişim izni almasını sağlayan bir kimlik doğrulama aracıdır. Token, erişim hakkı tanımlayan ve sınırlayan bir dizedir ve istemci tarafından kullanılarak korunan kaynaklara erişim sağlanır. Token'ın yapısı ve güvenlik seviyesi, **resource server**'ın güvenlik gereksinimlerine göre farklılık gösterebilir. Ancak temel amacı, kaynaklara erişimi yönetmek ve kimlik doğrulama işlemini daha verimli hale getirmektir.