2.1. Client Types bölümü, OAuth 2.0 protokolünde istemcilerin iki ana tipte sınıflandırıldığını açıklar. Bu sınıflandırma, istemcilerin yetkilendirme sunucusuyla güvenli bir şekilde kimlik doğrulaması yapabilme yeteneklerine dayanır. Temelde, istemcilerin kimlik bilgilerini (client credentials) gizli tutma kapasitesine göre iki ana türü belirlenmiştir:

1. Confidential Clients (Gizli İstemciler)

Confidential istemciler, kimlik bilgilerini güvenli bir şekilde saklayabilen ve yetkilendirme sunucusu ile güvenli bir şekilde kimlik doğrulaması yapabilen istemcilerdir. Bu istemciler, genellikle güvenli bir sunucu üzerinde çalışır ve istemci kimlik bilgilerine yalnızca kısıtlı erişimi olan uygulamalar tarafından erişilebilir.

- Örnek: Web uygulamaları, API istemcileri veya sunucu tarafı uygulamaları.
- Güvenlik: Bu istemciler, kimlik bilgilerini (client credentials) saklamak ve bunları güvenli bir şekilde kullanmak için gereken altyapıya sahiptir. Bu nedenle, bu tür istemciler daha güvenli kabul edilir.

2. Public Clients (Açık İstemciler)

Public istemciler, kimlik bilgilerini güvenli bir şekilde saklayamayan istemcilerdir. Bu istemciler, genellikle kullanıcının cihazında çalışan uygulamalardır (örneğin, yerel uygulamalar veya web tarayıcısında çalışan uygulamalar). Bu tür istemciler, kimlik bilgilerini güvenli bir şekilde saklayamazlar çünkü istemci kodu, kullanıcıya açık bir şekilde dağıtılır ve kullanıcıya veya cihazdaki diğer uygulamalara erişilebilir.

- Örnek: Yerel uygulamalar (native applications), web tarayıcı tabanlı uygulamalar.
- Güvenlik: Bu istemcilerde, kimlik bilgileri genellikle uygulama içinde açıkça saklanır, bu da güvenlik risklerine yol açabilir. Bu tür istemciler, genellikle kimlik doğrulaması için başka güvenlik önlemleri (örneğin, kullanıcının kimliği doğrulandıktan sonra kısa süreli erişim jetonları kullanma) gerektirir.

3. Client Type Belirlenmesi

İstemci türü, yetkilendirme sunucusunun güvenli kimlik doğrulama tanımına ve istemci kimlik bilgilerini açıklamaya karşı kabul edilebilir seviyesine dayanır. Yetkilendirme sunucusu, istemci türü konusunda varsayımlar yapmamalıdır, yani her istemci türünün güvenlik gereksinimleri farklıdır ve her birine uygun şekilde yaklaşılmalıdır.

4. Dağıtık İstemciler

Bir istemci, birden fazla bileşen içeriyor olabilir ve her bileşenin farklı bir istemci türü ve güvenlik bağlamı olabilir. Örneğin, bir dağıtık istemci hem gizli istemci bileşenlerine (sunucu tabanlı) hem de açık istemci bileşenlerine (tarayıcı tabanlı) sahip olabilir. Eğer yetkilendirme sunucusu bu tür istemcileri desteklemiyorsa, her bileşen ayrı bir istemci olarak kaydedilmelidir.

5. OAuth 2.0 İstemci Profilleri

OAuth 2.0, farklı istemci türleri için spesifik profiller tanımlar:

- **Web Application (Web Uygulaması)**: Bu, bir **confidential client** (gizli istemci) olup, web sunucusunda çalışır. Kaynak sahipleri, bu istemciye HTML kullanıcı arayüzü aracılığıyla

erişir. İstemci kimlik bilgileri ve erişim jetonları yalnızca web sunucusunda saklanır ve kaynak sahibine veya diğer kullanıcı ajanlarına (örneğin, tarayıcılar) erişilebilir değildir.

- **User-Agent-Based Application (Kullanıcı Ajansı Tabanlı Uygulama)**: Bu, bir **public client** (açık istemci) olup, istemci kodu bir web sunucusundan indirilir ve kullanıcı ajanı (örneğin, web tarayıcısı) üzerinde çalıştırılır. Bu tür istemcilerde, kimlik bilgileri ve protokol verileri kaynak sahibi tarafından kolayca erişilebilir ve genellikle görünürdür. Ancak, kullanıcı ajanının özellikleri, yetkilendirme talebinde bulunurken yardımcı olur.
- **Native Application (Yerel Uygulama)**: Bu da bir **public client** olup, kaynak sahibinin cihazına kurulur ve çalıştırılır. Bu tür istemcilerde, protokol verileri ve kimlik bilgileri erişilebilir, ancak uygulama tarafından kullanılan dinamik olarak verilen kimlik bilgileri (örneğin, erişim jetonları) kabul edilebilir seviyede korunabilir. Bu tür kimlik bilgileri, kötü niyetli sunuculardan korunduğu gibi, bazen cihazdaki diğer uygulamalardan da korunabilir.

6. Özet

OAuth 2.0, istemcileri **gizli** ve **açık** olarak iki ana kategoride sınıflandırır. **Gizli istemciler**, kimlik bilgilerini güvenli bir şekilde saklayabilirken, **açık istemciler** bunu yapamaz ve genellikle daha yüksek güvenlik önlemleri gerektirir. OAuth 2.0, farklı istemci türleri için güvenlik gereksinimlerini ve uygulama senaryolarını dikkate alarak, her tür için uygun çözümler sunar.