GTÜ OAuth Servisleri v1.0 Geliştirici Kılavuzu – Taslak - 1

1. **Amaç ve Kapsam**

   Kampüs SSO projesi aşağıdaki amaçlarla geliştirilmektedir:

   - GTÜ Bilgi İşlem Daire Başkanlığı (BİDB) kapsamında gerçekleştirilen otomasyon projeleri için bir ortak platform oluşturmak,
   - Bu projelere GTÜ şifresi ve E-Devlet logini ile SSO sağlamak,
   - Yetkilendirilmiş diğer projelere Oauth altyapısı ile güvenli login sağlamaktır

   Oauth, yetkilendirilmiş uygulamalara servis sağlayıcının ara yüzü üzerinden uygulamanın ihtiyaç duyduğu bilgilerle beraber güvenli bir biçimde login sağlamak için geliştirilmiş bir sistematiktir.

   Bu belge GTÜ Oauth servislerinin, bu servisleri kullanmak için yetkilendirilmiş uygulamalar tarafından kullanılabilmesi için yazılmış bir geliştirici kılavuzudur.

2. **Belirlenen Parametreler**

   Servislerden faydalanabilmek için uygulama üreticisi GTÜ BİDB'ye aşağıdaki parametreleri sağlar:

   redirect_uri. Yetkilendirme sunucusunun kullanıcıyı yönlendireceği uygulama sunucusunun kontrolündeki URL.
   Başlangıç noktası. Kullanıcının yönlendirilmesi durumunda uygulamanın Oauth sürecini başlatacağı adres. Bu adres Kampüs otomasyonu tarafından kullanıcının uygulamaya yönlendirilebilmesi için kullanılır.

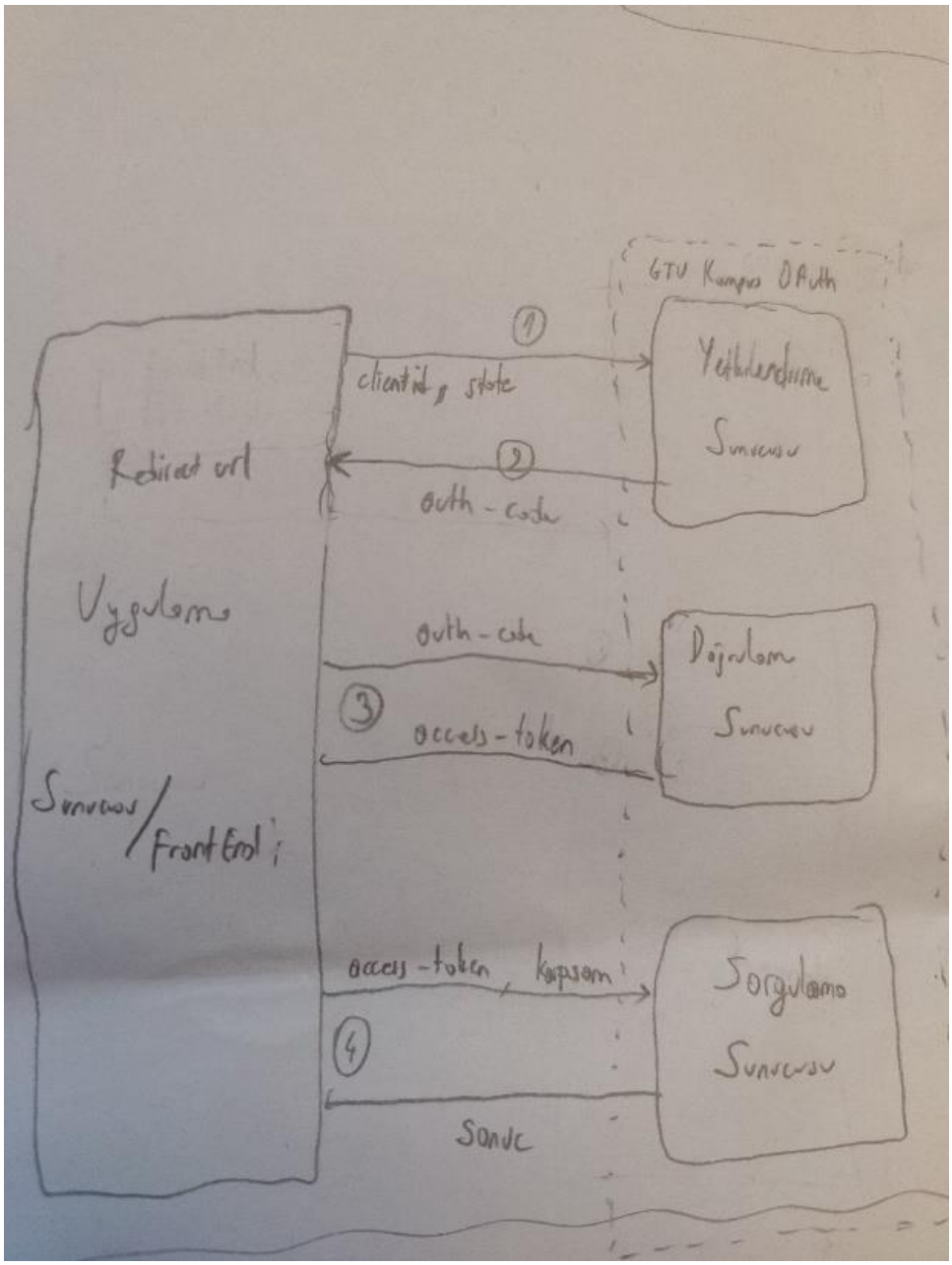
   GTÜ BİDB yetkilendirilmiş uygulamaya aşağıdaki bilgileri sağlar:

   client_id. Uygulamaya özel bir kimlik bilgisidir.
   client_secret. Uygulamaya özel verilen bir şifredir.

3. **Servis Adresleri**

   Yetkilendirme Sunucusu: https://kampus.gtu.edu.tr/oauth/yetki
   Doğrulama Sunucusu: https://kampus.gtu.edu.tr/oauth/dogrulama
   Sorgulama Sunucusu: https://kampus.gtu.edu.tr/oauth/sorgu

4. **Oauth Servislerinin Genel Yapısı**



Oauth hizmetleriyle ilgili akış ana hatlarıyla sırasıyla aşağıdaki gibidir:

- Yetkilendirilmiş uygulama son kullanıcıyı GTÜ Kampüs yetkilendirme sunucusuna gerekli parametrelerle yönlendirir (1. adım)
- Kullanıcı yetkilendirme sunucusunda login olur.
- Kullanıcı yetkilendirme sunucusu tarafından **redirect_uri** adresine **authorization_code** parametresiyle yönlendirilir (2. adım).
- Uygulama **authorization_code** ve kendisine sağlanan login bilgileriyle doğrulama sunucusundan **access_token** alır (3. adım).
- Uygulama **access_token**'ı kullanarak sahip olduğu yetkiler dâhilinde sorgulama sunucusundan kullanıcı ile ilgili bilgileri elde eder (4. adım).
- Uygulama kullanıcının login işlemini gerçekleştirir.

5. İşlem Adımlarının Detayları

5.1. Kullanıcının Yetkilendirme Sunucusuna Yönlendirilmesi

Uygulama kullanıcıyı aşağıdaki parametrelerle yetkilendirme sunucusuna yönlendirir:

response_type: "code" sabit değeri gönderilmeli

client_id: BİDB tarafından uygulamaya sağlanan değer

redirect_uri: Uygulama tarafından BİDB'ye bildirilen değer.

state: Login talebine özel üretilen rasgele bir kod. Bu kod bir sonraki adımda kontrol edilmek üzere kaydedilmeli.

code_challenge_method: "s256" sabit değeri gönderilmeli

code_challenge: 5.3'te belirtilen code_verifier'dan code_challange_method alanında belirtilen algoritma ile üretilen hash code. Bu kod adres satırından gönderilmesi gerektiği için Base64'e çevrilip percent encoding uygulanmalıdır. Code_challenge=PERCENT_ENCODE(BASE64_ENCODE(SHA256(code_verifier)))

örnek yönlendirme adresi:
https://kampus.gtu.edu.tr/oauth/yetki?response_type=code&client_id=xxxxx
&redirect_uri=https://uygulama.gtu.edu.tr/login/oauthredirect&state=random_value&
code_challenge_method=s256&code_challange=xxxxxxxxxx

5.2. Kullanıcının uygulamanın redirect_uri adresine yönlendirilmesi

Başarılı login sonrasında yetkilendirme sunucusu kullanıcıyı uygulamanın ilgili adresine aşağıdaki parametrelerle yönlendirir:

state: Bir önceki adımdaki state değeri geri gönderilir. Bu değer güvenlik amaçlı kontrol edilmeli ve kullanıcının bir önceki adımda uygulamanın kendisi tarafından yönlendirilmiş olduğundan emin olunmalıdır.
code: access_token alırken kullanılacak olan authentication_code değeri. Bu değer 20 saniye boyunca geçerlidir.

örnek yönlendirme adresi:
https://uygulama.gtu.edu.tr/login/oauthredirect?state=random_value&code=xxxxxxx

5.3. access_token alınması

HTTP Post kullanılarak doğrulama sunucusundan aşağıdaki parametreler **gövde üzerinden gönderilerek (from body)** access_token talep edilir:

client_id: BİDB tarafından uygulamaya sağlanan değer
client_secret: BİDB tarafından uygulamaya sağlanan değer
code: authentication_code değeri
code_verifier: Random olarak 43 ile 128 karakter arasında üretilen string değer (A-Z, a-z, 0-9 ve -._~ karekterleri kullanılabilir.).

Yanıt (Başarılı Durum):
{"access_token":"e083cdae16ff5fdac67e2872c15c0"}

Yanıt (Hatalı Durum):

```
{
    “error” : ”GKL_202”,
    “error_description” : “Geçersiz auth_code.”
}
```

access_token değeri 3 dakika boyunca kullanılabilir.

5.4. Sorgulama

Yetkili uygulama **HTTP Post** kullanılarak sorgulama sunucusundan aşağıdaki parametreleri **gövde üzerinden göndererek (from body)** yetkisi dahilinde aşağıdaki sorgulamaları yapabilir. Başarısız durumda 5.3’te belirtildiği gibi bir yanıt verilir.

Gönderilecek Parametreler (from body):
client_id: BİDB tarafından uygulamaya sağlanan değer
access_token
kapsam: Sorgulama tipini ifade eder

5.4.1. **Genel Servis**

kapsam parametresi “**GENEL**” olarak gönderilir.

Yanıt (Başarılı Durum):

kimlik_no_unique_id: kişiye özel üretilen bir benzersiz kod

kullanici_adi: kişinin loginde kullandığı GTU kullanıcı adı

kurumsal_email_adresi

ad

soyad

cinsiyet: “ERKEK” / ”KADIN”

kurum_ici: “TRUE” / “FALSE”

ogrenci: “TRUE” / “FALSE”

akademik_personel: “TRUE” / “FALSE”

idari_personel: “TRUE” / “FALSE”

5.4.2. **TC Kimlik Numarası Servisi**

kapsam parametresi “**`TC_KIMLIK_NO`**” olarak gönderilir.

Yanıt (Başarılı Durum):

kimlik_no: kişinin TC kimlik numarası

5.4.3. **Öğrencilik Servisi**

Kişinin temel öğrencilik bilgilerini getirir (henüz hazır değil

5.4.4. **Telefon Servisi**

Kişinin kayıtlı telefon bilgilerini getirir (henüz hazır değil)