جمهوری اسلامی ایران
وزارت بهداشت، درمان و آموزش پزشکی

سند راهنمای فنی اتصال سامانه های وزارت بهداشت به پنجره واحد خدمات سلامت

شناسه سند: Behdasht_SSO_TechnicalGuide_V.02

تاریخ آخرین تغییرات: ۱۴۰۲/۰۵/۳۱

چکیده: این سند حاوی راهکار فنی اتصال سامانه‌های ارائه دهنده خدمت وزارت بهداشت از طریق پنجره واحد خدمات وزارت بهداشت به پنجره ملی خدمات دولت هوشمند می‌باشد.

مرکز مدیریت آمار و فناوری اطلاعات وزارت بهداشت، درمان و آموزش پزشکی
تهران، شهرک قدس، خیابان سیمای ایران، بین فلامک و زرافشان، ستاد مرکزی وزارت بهداشت، درمان و آموزش پزشکی

تاریخچه

اصلاحیه	تاریخ	شرح
۱	۱۴۰۲/۰۴/۰۱	نسخه اولیه
۲	۱۴۰۲/۰۵/۳۱	بروز رسانی وب سرویس پروفایل

فهرست مطالب

۱. مقدمه

به منظور ایجاد بستر احراز هویت کاربران با استفاده از یک نام کاربری و کلمه عبور در تمامی سامانه‌های متمرکز در سازمان از ورود یکپارچه کاربران یا احراز هویت متمرکز (SSO[۱]) استفاده می‌گردد. با استفاده از این روش، احراز هویت کاربران به صورت متمرکز از یک نقطه انجام شده و پس از آن، داده‌های هویتی فرد در اختیار سامانه‌ها و سرویس‌های استفاده کننده قرار می‌گیرد.

از طرفی بر اساس ضوابط اجرایی دولت الکترونیکی، پنجره واحد خدمات سلامت با هدف تجمیع خدمات حوزه وزارت بهداشت و تسهیل دسترسی عموم مردم به این خدمات در دستور کار قرار گرفته است که در کنار قابلیت استفاده از SSO ارائه خدماتی مطلوب را برای کاربران در پی خواهد داشت؛ در راستای یکپارچه‌سازی با پنجره ملی خدمات دولت هوشمند، امکان ورود از طریق SSO دولت نیز وجود خواهد داشت.

بر این اساس تمامی مراکز تحت نظر وزارت بهداشت که سرویس‌های عمومی به مردم ارائه می‌دهند از طریق پنجره واحد خدمات سلامت، به پنجره ملی خدمات دولت هوشمند متصل خواهند شد.

۲. تعاریف و اصلاحات

پنجره ملی خدمات دولت هوشمند: سامانه my.gov.ir که امکان دسترسی به خدمات دولت را در قالب پیشخوان یکپارچه فراهم می‌نماید و برای استفاده سامانه‌های متصل به آن سرویس SSO را ارائه می‌دهد.

سرویس احراز هویت مرکزی وزارت بهداشت: این سرویس url آن در اختیار سامانه های مراکز تحت نظر وزارت بهداشت قرار خواهد گرفت و از این به بعد SSO نامیده می‌شود، مسئول پیاده‌سازی سیاست‌ها و استانداردهای احراز هویت مرکزی و کنترل دسترسی به سامانه‌های مختلف تحت نظارت وزارت بهداشت است.

پنجره واحد خدمات سلامت وزارت بهداشت: سامانه‌ای است که با آدرس my.behdasht.gov.ir در دسترس می‌باشد و وظیفه دسترسی یکپارچه به خدمات حوزه وزارت بهداشت را بر اساس ضوابط اجرایی پیاده‌سازی پنجره ملی خدمات دولت هوشمند برعهده دارد.

سامانه متقاضی SSO: سامانه ارائه دهنده خدمات در هر مرکز تحت نظارت وزارت بهداشت مانند دانشگاه‌ها و بیمارستان‌ها و ... که در قالب یک سامانه یا پنجره واحد می‌باشد و قرار است به سرویس احراز هویت مرکزی

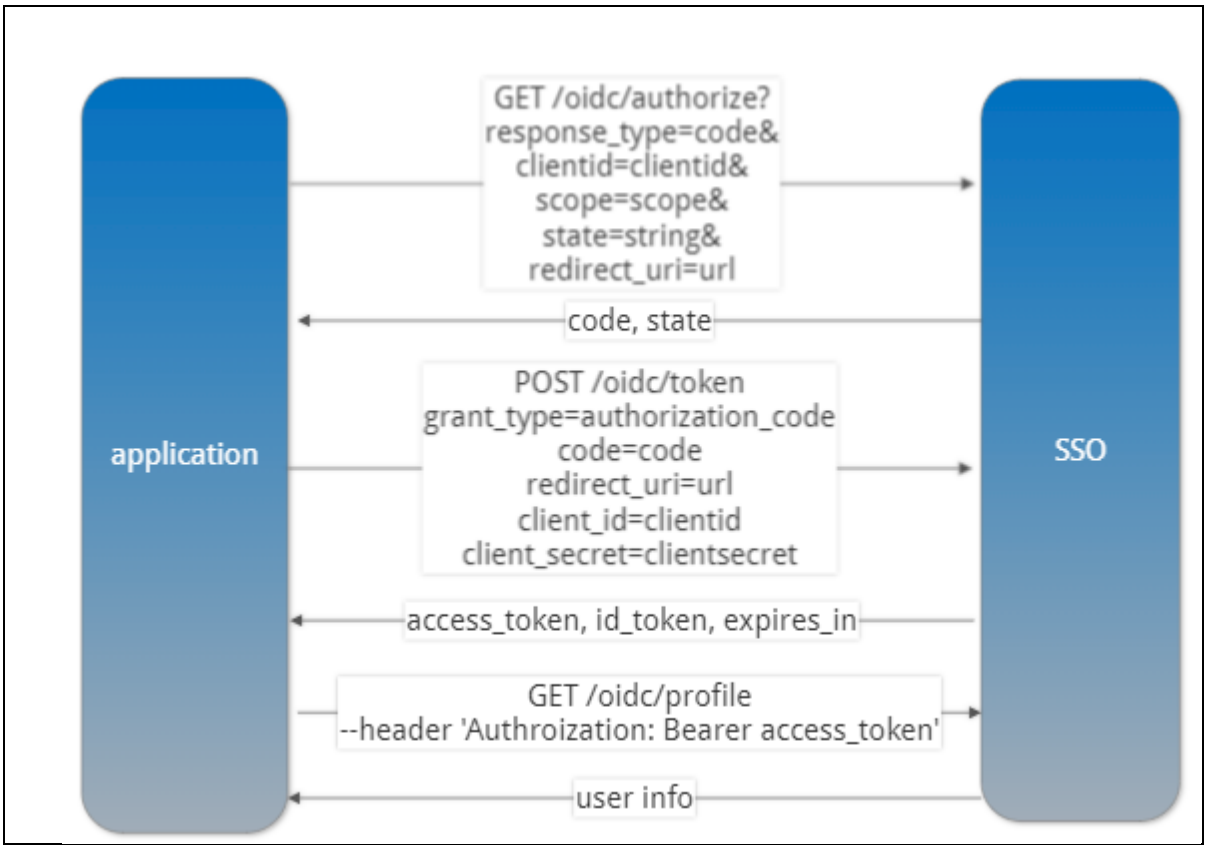
---

[۱] SSO (Single Sign On)

وزارت بهداشت متصل شود. در این سند در قسمت راهنمای فنی با نام application به آن اشاره می شود.

۳. سرویس احراز هویت متمرکز وزارت بهداشت

در این بخش راهنمایی لازم برای نحوه اتصال سامانه‌های تحت نظارت وزارت بهداشت به سرویس احراز هویت مرکزی این وزارتخانه ارائه شده است. این سرویس به‌صورت واسط بین پنجره واحد خدمات دولت هوشمند و سامانه‌های متقاضی SSO عمل می‌کند.



شکل ۱- ساز و کار احراز هویت کاربران

در ابتدا، سناریوی کلی تبادل اطلاعات بین سرویس احراز هویت مرکزی وزارت بهداشت و هر سامانه متقاضی SSO که از این به بعد application نامیده می‌شود، ارائه می‌گردد. سپس جزئیات تعریف پیام‌ها و داده‌های ارسالی به تفصیل شرح داده خواهد شد.

این سناریو با توجه به شکل ۱ به این صورت است:

- هنگامی که کاربر "ورود از پنجره واحد خدمات سلامت" را انتخاب کند، درخواست authorize توسط application به sso ارسال می‌گردد و در صورت تایید داده‌های دریافت شده توسط sso، به کاربر صفحه ورود پنجره ملی خدمات دولت هوشمند نمایش داده می‌شود.

- پس از ورود موفقیت آمیز کاربر، یک code موقت با اعتبار ۳۰ ثانیه به سمت application باز می‌گردد.

- در این زمان application باید code را همراه با سایر دیتاهای مشخص شده در دیاگرام برای وب سرویس token در sso ارسال کند تا توکن مرتبط با کاربر وارد شده با انقضای زمانی مشخص را دریافت کند. در صورت تایید داده‌های دریافتی توسط sso، مقادیر access_token, id_token و expires_in برای application ارسال می‌گردد. مقدار id_token یک توکن با استاندارد jwt است. مقدار access_token یک رشته تصادفی مرتبط با کاربر وارد شده با شروع AT است که برای دریافت سایر اطلاعات کاربر از وب سرویس profile استفاده می‌شود. مقدار expires_in مشخص کننده انقضای زمانی توکن دریافتی از sso می‌باشد. در صورت نیاز به صحت سنجی امضای توکن می‌توانید از آدرس زیر استفاده نمایید:

https://*sso_url*/oidc/jwks

- فراخوانی وب سرویس profile به منظور دریافت دیتای کاربر وارد شده از sso بر اساس مقادیر مجاز تعریف شده برای هر application می‌باشد. فراخوانی این سرویس با سرآیند Authtorization از نوع Basic است که نام کاربری و کلمه عبور آن به ترتیب client_id و client_secret دریافتی از وزارت بهداشت است و مقدار access_token دریافت شده از وب سرویس /oidc/token به صورت q param ارسال می‌گردد.

در صورتی که تمامی مراحل به درستی انجام شوند، بر اساس redirect_url تعریف شده، یک نشست برای کاربر با توکن دریافت شده در application ایجاد می‌شود.

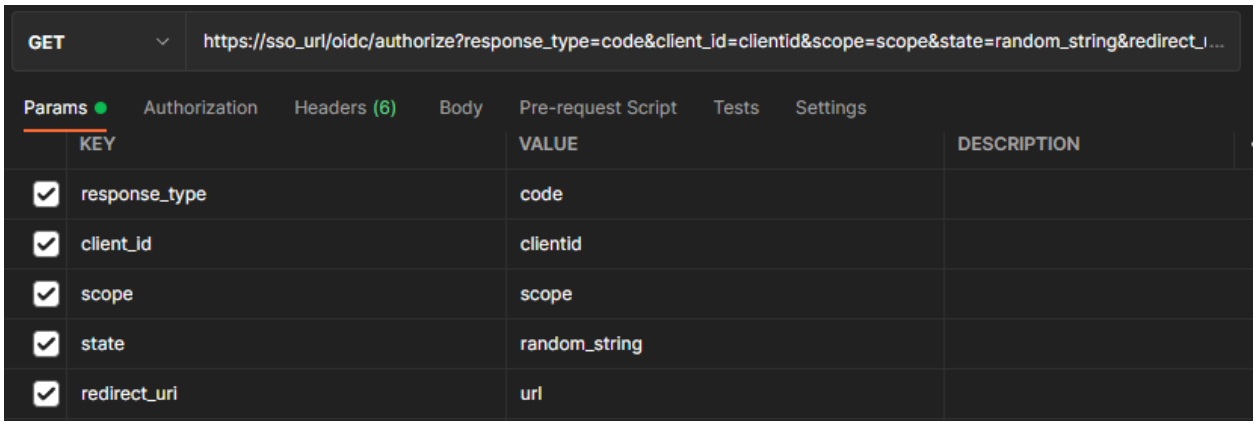
لازم به توضیح است که آدرس host سامانه sso (*sso_url*) و مقادیر یکتا و اختصاصی هر application از جمله client_id و client_secret و... پس از دریافت تاییدیه از وزارت بهداشت در اختیار مدیر/توسعه‌دهندگان سامانه متقاضی SSO قرار خواهد گرفت.

۴.نمونه فراخوانی وب سرویس‌ها در نرم افزار postman

نمونه فراخوانی وب سرویس‌های مشخص شده در دیاگرام شکل ۱ و سایر وب سرویس‌ها در ادامه شرح داده خواهند شد.

۴-۱.درخواست authorize

نمونه درخواست:



شکل ۱-نمونه درخواست authorize

GET
/oidc/authorize?response_type=code&client_id=clientid&scope=scope&state=random_string&redirect_uri=url

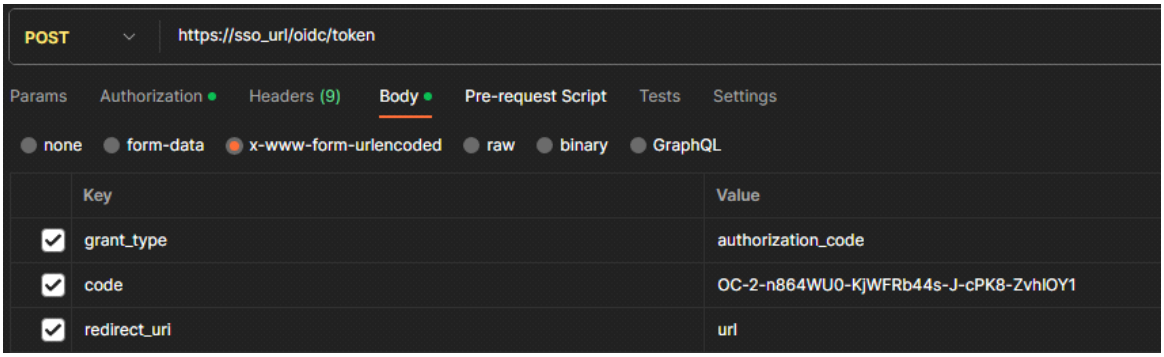
این درخواست باید هنگامی که کاربر گزینه ورود از طریق درگاه دولت را انتخاب می‌کند، از طرف application به sso ارسال گردد و پس از آن سامانه sso کاربر را به صفحه ورود هدایت می‌کند. در نظر داشته باشید که مقدار redirect_uri همان مسیر ورود کاربر بعد از احراز هویت در application است که مجوز آن توسط وزارت بهداشت

تایید می‌گردد. در صورتی که نام کاربری و کلمه عبور به درستی وارد شود، در پاسخ سامانه sso مقدار code و state را به application برمی‌گرداند. مقدار state یک رشته تصادفی به منظور ملاحظات امنیتی است و application باید مقدار بازگشتی با مقدار ارسالی را مطابقت دهد و در صورتی که مقادیر یکسان نباشند، فرآیند احراز هویت را متوقف نماید. مقدار response_type برابر با code می‌باشد و سایر مقادیر پس از تایید سامانه در وزارت بهداشت، در اختیار توسعه دهنده قرار خواهد گرفت.

همانطور که قبلا گفته شد، به مدت ۳۰ ثانیه application فرصت دارد تا وب سرویس token را فراخوانی کند و مقادیر access_token و id_token را دریافت نماید.

۲-۴.وب سرویس token

نمونه درخواست:



شکل۲ - نمونه درخواست وب سرویس token

POST /oidc/token

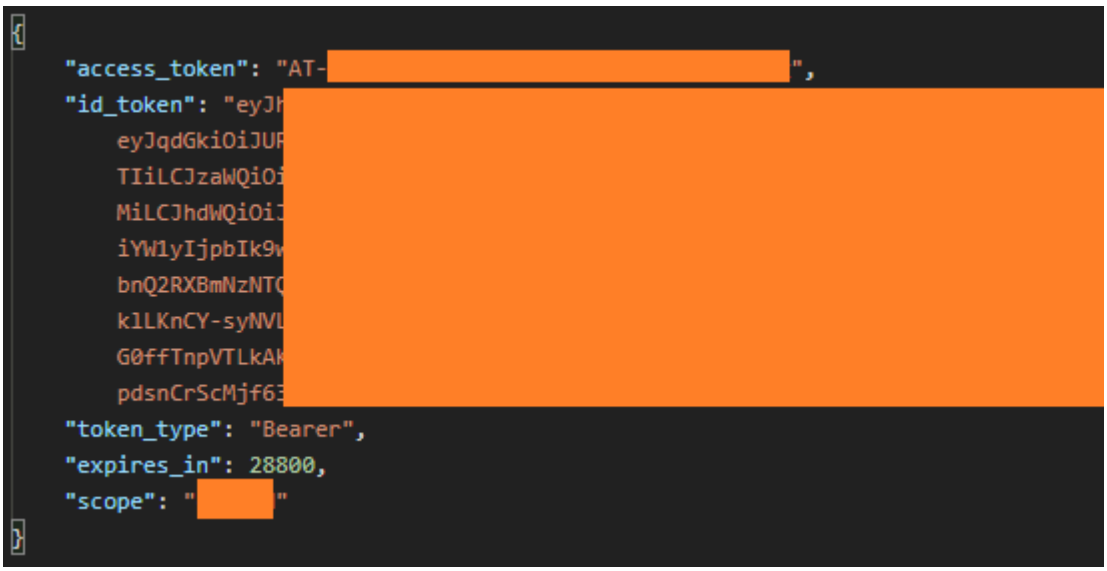
Host: *sso_url*

Authorization: Basic Y2xpZ…

Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&code=code&redirect_uri=url

نمونه پاسخ:



شکل۳ - نمونه پاسخ وب سرویس token

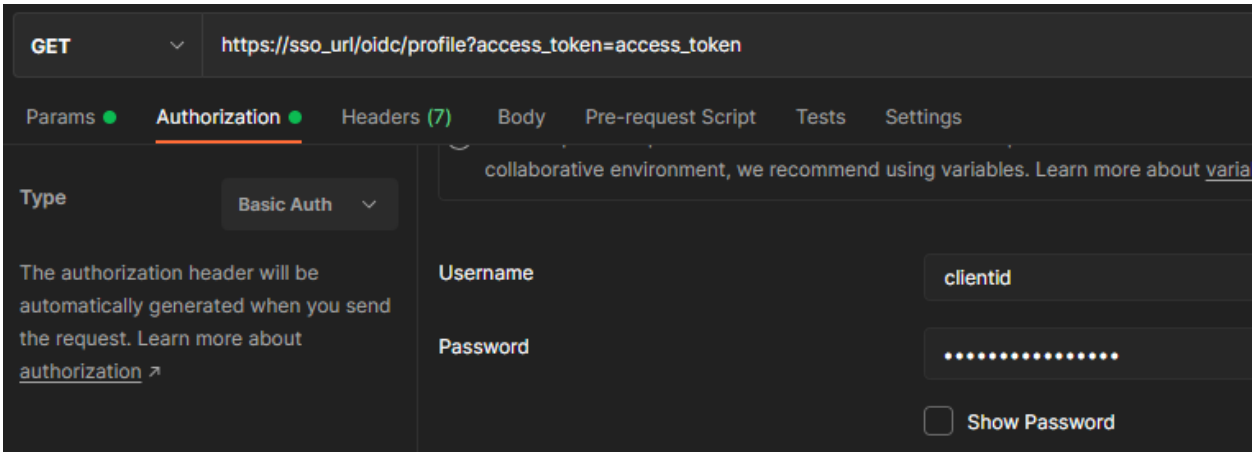
همانطور که ملاحظه می‌گردد، در صورت صحت دیتای ارسالی به وب سرویس، مقادیر به سمت application بازگردانده می‌شود. مقدار id_token بر اساس استاندارد jwt است که در وب سایت jwt.io امکان decode کردن این مقدار و مشاهده مقادیر موجود در id_token وجود دارد.

۳-۴.وب سرویس profile

به منظور مشاهده دیتای تکمیلی کاربر که توسط sso در scope هر سامانه تعریف می‌شود، با فراخوانی وب سرویس profile امکان پذیر می‌باشد. به این منظور بایستی مقادیر client_id و client_secret به صورت Basic

در Authorization header وب سرویس قرار گیرد و مقدار access_token دریافتی از وب سرویس token به صورت q param ارسال گردد.

نمونه درخواست:



شکل۴ - نمونه درخواست وب سرویس profile

GET /oidc/profile?access_token=access_token

Host: *sso_url*

Authorization: Basic Y2xpZ…

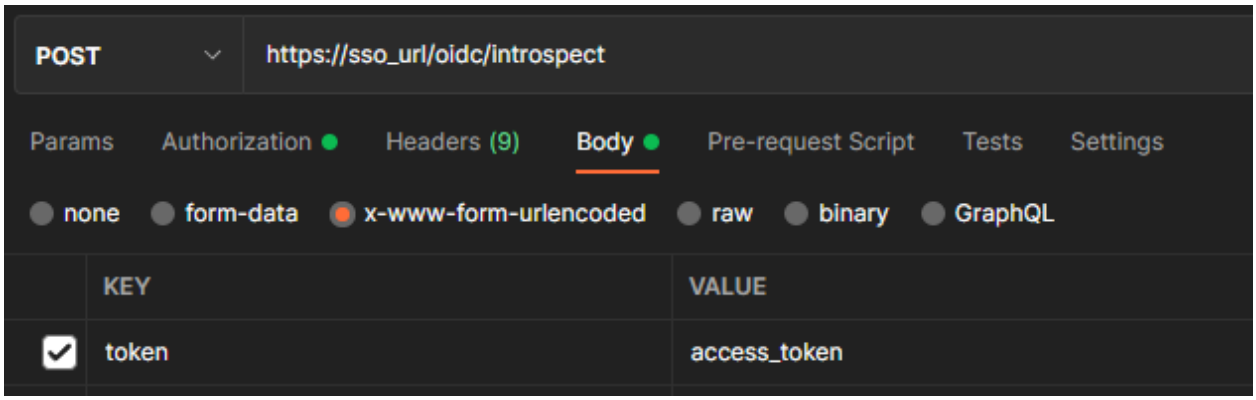
نمونه پاسخ:

شکل ۶- نمونه پاسخ وب سرویسprofile

۴-۴.وب سرویس introspect

به منظور صحت سنجی و بررسی وضعیت token کاربر از وب سرویس introspect استفاده می‌شود. به این منظور بایستی مقادیر client_id و client_secret به صورت Basic در Authorization header وب سرویس قرار گیرد و مقدار access_token دریافتی از وب سرویس token در بدنه وب سرویس ارسال شود.

نمونه فراخوانی:



شکل ۵ – نمونه فراخوانی وب سرویس introspect

POST /oidc/introspect

Host: *sso_url*

Authorization: Basic Y2xp…

Content-Type: application/x-www-form-urlencoded

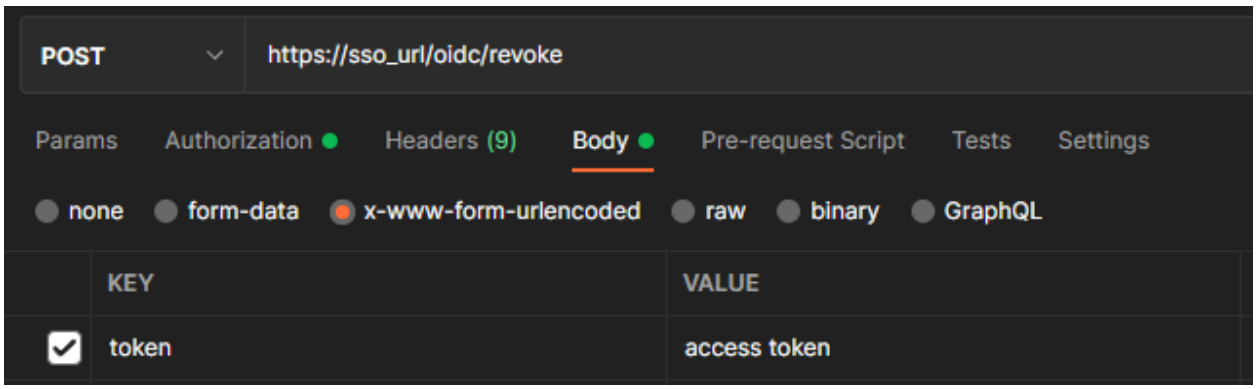
token=access_token

مقدار active در خروجی این وب سرویس نشان دهنده معتبر یا غیر معتبر بودن token کاربر می‌باشد.

۵-۴.وب سرویس revoke

اگر به هر دلیلی application تصمیم بگیرد token کاربر را قبل از رسیدن به زمان خاتمه آن، منقضی کند، می‌توان با فراخوانی وب سرویس revoke این امر را محقق نمود. به این منظور بایستی مقادیر client_id و client_secret به صورت Basic در Authorization header وب سرویس قرار گیرد و مقدار access_token دریافتی از وب سرویس token در بدنه وب سرویس ارسال شود.

نمونه درخواست:



شکل ۶ – نمونه فراخوانی وب سرویس revoke

POST /oidc/revoke

Host: *sso_url*

Authorization: Basic Y2xpZ…

Content-Type: application/x-www-form-urlencoded

token=access_token

در صورتی که عملیات منقضی کردن توکن با موفقیت انجام شود مقدار http_response_code برابر با ۲۰۰ به سمت application بازگردانده می‌شود. جهت اطمینان بیشتر با فراخوانی مجدد وب سرویس introspect مشاهده خواهد شد که مقدار active برای access_token ارسالی برابر با false شده است.

در هریک از مراحل شرح داده شده، ممکن است خطاهایی رخ دهد که شرح آن مطابق جدول زیر می‌باشد:

خطای دریافتی	علت
"error": "invalid_grant"	• شرایطی که مقدار code ارسالی به وب سرویس token نامعتبر باشد، مثلا استفاده مجدد از یک کد صورت گیرد و یا درخواست token بعد از ۳۰ ثانیه از دریافت کد انجام شود. • اگر client_id و redirect_uri درخواست authorize نادرست باشند.
"error": "expired_accessToken"	در صورتی مقدار access_token ارسالی به سرویس profile منقضی شده باشد
"error": "missing_accessToken"	درصورتی access_token به وب سرویس profile ارسال نشود.

پایان