سازمان فناوری اطلاعات ایران

وزارت ارتباطات و فناوری

راهنمای اتصال نهادهای متکی به سامانه سماوا

(سامانه احراز هویت معتبر در فضای مجازی)

ویرایش: مهرماه ۱۳۹۹

تهیه‌کننده: اداره کل توسعه خدمات دولت الکترونیکی

اداره پیش‌بینی و احصاء خدمات الکترونیکی

(هرگونه کپی‌برداری از این سند منوط به کسب اجازه کتبی از سازمان فناوری اطلاعات ایران است)

سازمان فناوری اطلاعات ایران

فهرست مطالب

سازمان فناوری اطلاعات ایران

مقدمه

سامانه سماوا، سامانه‌ای است برای احراز هویت و استعلام اشخاص. این سرویس در اختیار کسب و کارها قرار می‌گیرد تا بخشی از شناخت کاربران که نیازمند ارتباط با بانک‌های اطلاعاتی حاکمیتی است به واسطه آن انجام شود. در این فرآیند زمانی که نیاز به این شناسایی به وجود می‌آید، کاربر از طریق سامانه (سایت یا اپلیکیشن) کسب و کار، به صفحه سماوا هدایت (redirect) می‌شود. پس از شناسایی و استعلام موفق، کاربر از صفحه سماوا به سایت کسب و کار بازگردانده می‌شود و توکنی در اختیار کسب و کار قرار می‌گیرد که باید متناظر با کاربر آن را نگهداری کند. این توکن تا قبل از زمان انقضاء، معتبر است و نیازی نیست در مراجعات بعدی کاربر به کسب و کار این فرآیند تکرار شود. تشخیص اتمام اعتبار توکن، و نیاز به دریافت توکن جدید برای هر کاربر توسط کسب و کارها صورت می‌گیرد. هر زمان مراجع ذی ربط نیازمند بررسی بیشتر باشند، کسب و کارها این توکن را در اختیار ایشان قرار خواهند داد.

سازمان فناوری اطلاعات ایران

آنچه قبل از شروع باید بدانیم

در زمان ثبت نام

در فرآیند ثبت نام، اطلاعاتی رد و بدل می‌شود که در فرآیند اصلی مورد استفاده قرار می‌گیرند. لذا خوب است قبل از ثبت نام این بخش را به دقت مطالعه بفرمایید.

اطلاعاتی که از کسب و کار ها در زمان ثبت نام دریافت می شود :

۱. نام کسب و کار : اسم رسمی شرکت (به فارسی)
۲. تصویر logo به فرمت png یا jpg : این تصویر باید مربوط به برند شما باشد. دقت کنید لوگوی شرکت مد نظر نیست. ارتفاع این عکس حداکثر ۶۴ پیکسل و حجم آن حداکثر K۵۰ باشد. دقت بفرمایید این تصویر در پس زمینه ای با رنگ سرمه ای تیره نشان داده خواهد شد. لذا جهت نمایش مناسب، لوگویی را ارسال کنید که ترکیب رنگ آن مطابقت بیشتری با این پس زمینه دارد.
۳. IP Valid: در فرآیند احراز هویت دو سرویس وجود دارد که از نهادهای متکی (سرور کسب و کارها) فراخوانی می‌شوند که بر روی آدرس این دو سرویس محدودیت اعمال شده‌است و فقط بر روی یک IP معتبر و ثابت از سوی کسب و کار پاسخ داده خواهد شد. لذا لازم است این IP در زمان ثبت نام اعلام شود.
۴. اطلاعات سرویس شاهکار :
    a. نام کاربری
    b. گذرواژه
    c. کد
۵. اطلاعات pgsb سرویس شاهکار :
    a. شناسه (client-id)
    b. رمز (client-secret)
    c. نام کاربری (pgsb-username)
    d. گذرواژه (pgsb-password)
    e. شناسه بسته (pid)
۶. آدرس‌های بازگشت (redirect_uri) : آدرسی در سامانه کسب و کار که در انتهای فرآیند احراز هویت، کاربر به آن هدایت می‌شود. دقت کنید در زمان ثبت نام کسب و کار می‌تواند بیش از یک مورد آدرس بازگشتی داشته باشد، اما در هر بار شروع فرآیند احراز هویت، فقط یکی از آدرس‌ها قابل ارسال می‌باشد (به صورت معمول هر

کسب و کار یک آدرس بازگشت دارد). در محیط تستی سامانه سماوا، نیازی نیست این آدرس بر بستر Https باشد ولی در محیط عملیاتی سماوا حتما باید آدرس بازگشت کسب و کار بر روی بستر Https قرار گرفته‌باشد.

۷. شماره موبایل : پس از ثبت اطلاعات کسب و کار در سامانه، پیامکی حاوی اطلاعات اتصال به سامانه که شامل client_id و client_secret می‌باشد به این شماره ارسال می‌شود. لازم به ذکر است که ارسال اطلاعات دو بار برای کسب و کار در محیط‌های تستی و عملیاتی سماوا انجام می‌شود

اطلاعاتی که به کسب و کارها پس از ثبت نام ارایه می شود:

۱. **شناسه کلاینت (client_id):** مورد استفاده در فرآیند توکن‌گیری

۲. **رمز کلاینت (client_secret):** مورد استفاده در فرآیند توکن‌گیری

در زمان توسعه

۱. شما ابتدا در یک محیط آزمایشی اقدام به ارتباط با سامانه سماوا خواهیدکرد و در صورت تایید این ارتباط توسط راهبران، باید آدرس‌های سامانه اصلی را با آدرس‌های سامانه آزمایشی در فراخوانی سرویس‌ها جایگزین نمایید.

۲. سامانه بر پایه استاندارد OAuth2 توسعه یافته است. لذا آشنایی با این استاندارد، توسعه دهنده را در درک راه حل و نحوه استفاده یاری می رساند (در صورت تمایل می توانید برای آشنایی کلی با OAuth2 پیوست 1 را مطالعه فرمایید).

۳. کسب و کارها می‌توانند در مراحل مختلف ارایه خدمت از سماوا استفاده‌کنند (برای مثال بعضی از کسب و کارها می‌توانند پس از ثبت‌نام کاربر در سامانه خود او را به سماوا هدایت‌کنند و بعضی دیگر در هنگام وقوع رخداد مهمی، مثل درخواست یک خدمت)

۴. درخواست صدور توکن بر پایه شماره تلفن همراه کاربر، به سماوا ارسال می‌شود. لذا توکن صادر شده مختص شماره تلفن همراه اعلامی است و نگهداری و تخصیص به کاربر مورد نظر باید به خوبی و با اطمینان بالا توسط کسب و کار توسعه یابد.

۵. این مساله بر عهده کسب و کار خواهد بود که اگر کاربری، دارای توکن معتبر نیست، وی را به سامانه سماوا هدایت‌کند. توکن معتبر، توکنی است که مقدار دارد، و زمان انقضای آن به اتمام نرسیده است. به یاد داشته باشید، در انتهای فرآیند، زمانی که توکن صادر می‌شود، به همراه آن، زمان ایجاد و طول عمر توکن نیز ارائه می‌شود. (توضیحات بیشتر در بخش "مرحله پنجم : سرویس درخواست توکن" همین سند)

۶. مراقبت‌های امنیتی و ایمنی را چه در نگهداری اطلاعات خصوصی (مانند شناسه و رمزی که در اختیار قرار می گیرد) و چه در محیط توسعه نرم افزار، بسیار حائز اهمیت هستند.

سازمان فناوری اطلاعات ایران

راهنمای مراحل احراز هویت سماوا (فرآیند دریافت توکن)

برای اتصال به سامانه سماوا و دریافت توکن برای هر کاربر، فرآیندی شامل مراحل زیر طراحی شده‌است. دقت کنید طی یک مرحله، کسب و کار شناسایی می‌شود و بعد از آن نوبت به شناسایی کاربر (مشتری یا خدمت گیرنده کسب و کار) می‌رسد :

- مرحله اول (شناسایی کسب و کار): سرویس شناسایی کسب و کار را فراخوانی می‌کنید و در صورت تایید، یک URL دریافت خواهید کرد.
- مرحله دوم (درخواست شناسایی کاربر): کاربر را به آدرسی که در مرحله قبل دریافت کردید هدایت (redirect) می‌کنید.
- مرحله سوم (عملیات شناسایی کاربر): برگزاری مراسم شناسایی کاربر در سامانه سماوا.
- مرحله چهارم (بازگرداندن کاربر به سامانه کسب و کار): هدایت کاربر به سامانه کسب و کار.
- مرحله پنجم (درخواست توکن): درخواست توکن از سماوا.

مرحله اول، دوم و پنجم توسط کسب و کار باید توسعه یابد.

نکات زیر را پیش از این نیز عارض شده ایم، اما به دلیل اهمیتی که دارند یک بار دیگر متذکر می شویم :

۱. به خاطر داشته باشید که توکن‌های دریافتی را باید ذخیره کنید و در صورت منقضی شدن، مجدد فرآیند توکن‌گیری برای کاربر را شروع کنید. البته ممکن است شما در مسند طراحی کسب و کار، دریافت مجدد توکن برای کاربر در صورت انقضا را به زمانی که کاربر درخواست جدیدی داشت موکول کنید. و یا در صورتی که در ارائه خدمت، زمان اهمیت دارد بلافاصله با انقضای توکن، کاربر را نسبت به دریافت مجدد توکن، رهنمون شوید. به عنوان مثال طراح در خرید اینترنتی، این مسأله را به زمانی واگذار می‌کند که کاربر درخواست خرید دارد. اما در درخواست تاکسی اینترنتی، شاید طراح لازم بداند زمان فرآیند درخواست و ارائه آن را کوتاه کند، بنابراین در صورت اتمام زمان توکن بلافاصله فرآیند توکن‌گیری مجدد را آغاز می‌کند. نتیجتاً مسأله مهم این است که کاربر بدون توکن معتبر و غیرمنقضی، خدمتی را از کسب و کار دریافت نکند.
۲. شما ابتدا باید در محیط آزمایشی اقدام به اتصال به سامانه سماوا کنید. پس از اتمام مراحل توسعه و تأیید راهبر سماوا، به شما اعلام می‌شود که اجازه اتصال به سامانه اصلی را دارید. در این مرحله کافی است آدرس‌های سامانه آزمایشی سماوا را در فراخوانی‌های خود، به آدرس‌های اصلی تغییر دهید.
۳. تنها می‌توانید از IP Valid که در زمان ثبت نام اعلام کرده‌اید، برای اتصال به سماوا استفاده کنید.

سازمان فناوری اطلاعات ایران

مرحله اول : شناسایی کسب و کار

در ابتدا باید درخواستی با مشخصات زیر بر روی آدرس پایه https://idtest.iran.ir ارسال کنید. در صورت تأیید اطلاعات ارسالی، پاسخی شامل URL مورد استفاده برای ه دایت کاربر در گام بعدی و کد امنیتی و آدرس پایه‌ای برگردانده می‌شود.

نمونه درخواست

نمونه درخواست

```
POST /oauth/create_authorize HTTP/1.1
Host: idtest.iran.ir
Content-Type: application/json
{
    "client_id": "test",
    "client_secret": "Ze0fve15W2RG03M5yl9At5bV2RGZJg84pI2V3ZrlmNyfIhX0",
    "scopes": ["mobile_number"],
    "redirect_uri": "https://iddemo.iran.ir/buy",
    "state": "d4a560fc-c4c2-11ea-87d0-0242ac130003",
    "loa": "LEVEL_2_2",
    "mobile_number":"09120000000"
}
```

شرح بدنه درخواست

نام فیلد	مقدار	جنس فیلد
client_id (شناسه)	شناسه کسب و کار که در زمان ثبت نام به شما داده شده‌است.	رشته
client_secret (رمز)	رمز کسب و کار که در زمان ثبت نام به شما داده شده‌است.	رشته
scopes (حوزه)	پس از ثبت‌نام، لیست حوزه‌های موردنیاز به کسب و کار داده می‌شود برای توضیحات بیشتر به بخش آخر مستند رجوع شود.	آرایه از نوع رشته
redirect_uri (آدرس بازگشت)	آدرسی که کاربر نهایی پس از فرآیند شناسایی به آن منتقل خواهد شد. این آدرس باید برابر با یکی از redirect-uriهای	رشته

نام فیلد	مقدار	جنس فیلد
	تعریف‌شده برای کسب و کار در زمان ثبت نام باشد.	
state (وضعیت)	رشته ای یکتا با طول حداقل ۳۲ کاراکتر است که در سامانه شما (کسب و کار) به ازای هر درخواست تولید می‌شود.	رشته
loa (سطح اطمینان)	مقدار ثابت LEVEL_2_2 را قرار دهید.	رشته
mobile_number (شماره موبایل)	پس از ثبت‌نام، اجباری بودن/نبودن این فیلد به کسب و کار اعلام می‌شود که البته با توجه به نیاز آن است . ۱. در صورت اجباری بودن این فیلد در صورت مشاهده نشدن آن در درخواست به کسب و کار خطا برگردانده می‌شود. ۲. در صورت اختیاری بودن این فیلد اگر در درخواست مشاهده‌نشود مشکلی ندارد ولی اگر مشاهده‌شود صحت‌سنجی بر روی آن رخ‌می‌دهد. کلا در هر دو حالت اجباری بودن/نبودن اگر شماره موبایلی در درخواست موجود و معتبر باشد آنگاه صحت‌سنجی کاربر در مرحله سوم فقط با همین شماره دریافتی امکان‌پذیر است. ولی اگر در حالت اختیاری بودن این فیلد، شماره موبایل در درخواست نباشد آنگاه کاربر در مرحله سوم باید شماره موبایلی وارد کند تا عملیات احرازهویت با شماره‌ی واردشده انجام پذیرد.	رشته

نمونه پاسخ (status=200)

```
{
    "authorize_url":
"https://idtest.iran.ir/oauth/authorize?client_id=test&scope=mobile_number&re
direct_uri=https%3A%2F%2Fiddemo.iran.ir%3A9000%2Fbuy&response_type=code&state
=d4a560fc-c4c2-11ea-87d0-0242ac130003",
    "b2b_base_url": "https://idtest.iran.ir",
    "secure_code": "KofxEBaEpPlM6lRnyhUC5kVAW7nuQwPV"
}
```

سازمان فناوری اطلاعات ایران

شرح بدنه پاسخ

نام فیلد	مقدار	جنس
authorize_url	آدرسی که کسب و کار در مرحله بعدی، کاربر را به آن هدایت می‌کند.	رشته
secure_code	کد امنیتی که باید آن را ذخیره کنید. (در مرحله پنجم آن را لازم داریم)	رشته
b2b_base_url	آدرس پایه برای سرویس‌های مرحله پنجم(سرویس دریافت توکن) و صحت‌سنجی می‌باشد. (آدرس پایه این سرویس‌ها به صورت داینامیک تبدیل شده‌است)	رشته

با شروع فرآیند احراز هویت، سامانه کسب و کار یک کد به نام state را ارسال کرده و یک کد به نام secure_codeدریافت می‌کند. با هر بار شروع فرآیند احراز هویت سماوا، کسب و کار باید این دو مقدار را به همراه زمان ایجاد state کنار یکدیگر تا پایان فرآیند نگهداری کند. جهت سهولت، در این سند این ذخیره‌سازی را «لیستstate ها» نام‌گذاری می‌کنیم.

فیلدی به نام b2b_base_url اضافه شده‌است که شامل آدرس پایه برای سرویس دریافت توکن و سرویس‌های صحت‌سنجی توکن می‌باشد. اما چون آدرس پایه این سرویس‌ها می‌تواند به صورت داینامیک تغییر کند، کسب و کار نیاز دارد همانطور که مانند عبارت بالا مقدار secure_code را با توجه به state در نزد خود نگه می‌دارد، مقدار آدرس b2b_base_url را نیز به همین شکل نگهداری‌کند تا در زمان فراخوانی سرویس‌های موردنظر از آن استفاده‌کند.

نمونه پاسخ‌های خطا

پیام تمام حالت‌های خطا در آرایه errors ذخیره می‌شود.

نمونه پاسخ(status=400)

حالتی که وضعیت (state) دریافت‌شده برای کسب و کار تکراری باشد، خطا نشان داده می‌شود و قادر به ادامه مراحل احراز هویت نخواهید بود .

حالتی که به جز فیلد client_id ، مقادیر سایر فیلدها نامعتبر باشند، نمونه پاسخ به شرح زیر خواهد بود:

نمونه پاسخ ۴۰۰

```
{
    "errors": [
        "اطلاعات هویتی به درستی وارد نشده‌است",
        "مقدار حوزه به درستی وارد نشده‌است",
        "مقدار آدرس بازگشت به درستی وارد نشده‌است",
        "طول رشته وضعیت کمتر از حد مجاز است",
        "مقدار سطح اطمینان به درستی وارد نشده‌است",
        "مقدار شماره موبایل به درستی وارد نشده‌است"
    ]
}
```

نمونه پاسخ(status=500)

نمونه پاسخ ۵۰۰

```
{
    "errors": [
        "مشکل داخلی به وجود آمده است"
    ]
}
```

سازمان فناوری اطلاعات ایران

مرحله دوم : سرویس درخواست شناسایی کاربر

در این مرحله باید کاربر را به آدرس authorize_url که از مرحله قبل دریافت کردید، هدایت (redirect) کنید.
البته این آدرس دارای محدودیت‌های زیر می‌باشد که باید به آن‌ها توجه داشته باشید.

۱. زمان مجاز برای استفاده: ۵ دقیقه
۲. تعداد دفعات مجاز برای استفاده: ۲ بار

سامانه سماوا با دریافت درخواست شناسایی کاربر تحت آدرس /oauth/authorize شروع به صحت‌سنجی اطلاعات ارسالی می‌کند.

۱) در صورت بودن معتبر بودن اطلاعات، شناسایی کاربر در سماوا ادامه پیدا می‌کند.
۲) در صورت نامعتبر بودن اطلاعات، به هر یک از دلایل زیر، کاربر صفحه خطا با ذکر دلیل را مشاهده خواهدکرد.
   a. زمان استفاده از این آدرس (authorize_url) به پایان رسیده باشد.
   b. از این آدرس (authorize_url) بیش از حد مجاز استفاده شده باشد.
   c. پارامترهای موجود روی درخواست نامعتبر باشند.

مرحله سوم : عملیات شناسایی کاربر در سماوا

در این مرحله شناسایی کاربر از طریق پیامک و سامانه شاهکار صورت می‌گیرد و در هر دو صورت موفق یا ناموفق بودن عملیات، کاربر به آدرس کسب و کار هدایت می‌شود (آدرسی که در redirect_uri تعیین شده بود).

۱. در حالت موفقیت‌آمیز: بر روی آدرس بازگشتی (redirect_uri) دو مقدار code و state به صورت پارامتر (query parameter) قرار می‌گیرد.
۲. در حالت ناموفق: بر روی آدرس بازگشتی (redirect_uri) دو مقدار error و state به صورت پارامتر (query parameter) قرار می‌گیرد که در پارامتر error دلیل خطای احراز هویت کاربر قرار داده شده‌است.

سازمان فناوری اطلاعات ایران

مرحله چهارم: بازگرداندن کاربر به سامانه کسب و کار

کاربر در این مرحله به آدرس کسب و کار(redirect_uri) بازگردانده می‌شود. همانطور که در مرحله پیش گفتیم، پارامتر state جزو پارامترهای پاسخ خواهند بود.

ابتدا باید صحت‌سنجی state را انجام دهید. یعنی:

۱. مطمئن شوید این پارامتر، در لیست stateهای شما (که در مرحله اول به آن اشاره شد) موجود است.
۲. زمان دریافت پاسخ را با زمان متناظر با این state در لیست stateها مقایسه کنید. فاصله این دو زمان باید کم‌تر از ۱۰ دقیقه باشد.

در صورت برقرار بودن دو شرط بالا:

- اگر روی پاسخ دریافت شده پارامتر error موجود بود، باید پیغام خطایی مبنی بر «با مشکل مواجه شدن فرآیند احراز هویت» به کاربر نشان دهید. در این حالت احراز هویت در همین مرحله به اتمام می‌رسد و مرحله پنجم انجام نخواهد شد.
- اگر روی پاسخ دریافت شده پارامتر code موجود بود، یعنی عملیات موفقیت‌آمیز بوده و از پارامتر code برای گام پنجم استفاده خواهید کرد.

در صورت برقرار نبودن دو شرط مذکور باید پیغام خطایی مبنی بر «با مشکل مواجه شدن فرآیند احراز هویت» به کاربر نشان دهید. در این حالت احراز هویت در همین مرحله به اتمام می‌رسد و مرحله پنجم انجام نخواهد شد.

سازمان فناوری اطلاعات ایران

مرحله پنجم : سرویس درخواست توکن

این سرویس بر روی آدرس پایه دریافتی از مقدار فیلد b2b_base_url در پاسخ مرحله اول قراردارد.

مقدار دریافت شده در پاسخ مرحله اول برابر با https://idtest.iran.ir می‌باشد که با توجه به آدرس خود این سرویس (یعنی /oauth/token) نمونه درخواست زیر با توجه به آن تولید شده‌است.

نمونه درخواست

نمونه درخواست

```
POST /oauth/token HTTP/1.1
Host: idtest.iran.ir
Authorization: Basic dGVzdDpkNGE1NjBmYy1jNGMyLTExZWEtODdkMC0wMjQyYWMxMzAwMDM=
Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code
&code=yL3wWgEgAoKb623uBDMxoQICjGQUVuAd
&secure_code=KofxEBaEpPlM6lRnyhUC5kVAW7nuQwPV
&redirect_uri=https://iddemo.iran.ir/buy
```

شرح سرآیند

نام سرآیند	مقدار	جنس
Authorization	یک رشته ثابت با مقدار: اطلاعات رمز شده کسب و کار + کاراکتر فاصله + "Basic" • **اطلاعات رمزشده کسب و کار**: در زمان ثبت نام، دو مقدار شناسه کلاینت (client_id) و رمز کلاینت (client_secret) به شما داده شده‌است. این دو رشته را به این ترتیب به هم‌دیگر الصاق کنید. • **client_id:client_secret** (به کاراکتر : بین این دو دقت کنید) و سپس با روش Base64 کد کنید. به سرآیند Authorization در نمونه درخواست بالا دقت کنید.	رشته

سازمان فناوری اطلاعات ایران

شرح بدنه درخواست

نام فیلد	مقدار	جنس
grant_type	مقدار ثابت "authorization_code"	رشته
code	در مرحله قبلی از روی پارامترهای پاسخ دریافت کرده‌اید.	رشته
secure_code	به لیست stateها مراجعه کنید. secure_code متناظر با state که در مرحله قبل دریافت کردید.	رشته
redirect_uri	آدرسی که در مرحله اول فرستاده شده‌است.	رشته

پیشنهاد: پس از فراخوانی این سرویس، اعتبار secure_code به پایان می‌رسد. لذا بهتر است جهت افزایش بهره‌وری، رکورد متناظر با state یا secure_code را از لیست state هایتان حذف کنید.

نمونه پاسخ

نمونه پاسخ موفقیت‌آمیز (status=200)


```
{
    "access_token":
"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJjcmVhdGlvbl90aW1lIjoidcpPph5jwYqgOz5
1aJEDBzpHNah-OY",
    "token_type": "bearer",
    "expires_in": 2764799,
    "scope": "mobile_number",
    "creation_time": "2020-07-13  16:08:44.132",
    "user_name": "09124958820",
    "jti": "53d846d6-d86f-42f0-afbc-c540c8aa1bba-01-2020-07-13",
    "loa": "LEVEL_2_2"
}
```

سازمان فناوری اطلاعات ایران

شرح پارامترها موجود در پاسخ موفقیت‌آمیز دریافت توکن

نام فیلد	مقدار	جنس
access_token	توکن صادر شده	رشته
token_type	مقدار ثابت "bearer"	رشته
expires_in	طول عمر توکن به ثانیه	عدد
scope	برابر با scope (حوزه‌های) ارسالی در درخواست مرحله اول	رشته
creation_time	زمان ایجاد توکن به فرمت yyyy-MM-dd HH:mm:ss.SSS	رشته
user_name	شماره موبایل کاربری که برای استعلام به سامانه معرفی شده است	رشته
jti	شمارنده یکتا متناظر با توکن است.	رشته
loa	مقدار ثابت "LEVEL_2_2"	رشته

فیلدهای دیگری نظیر national_number و person_identifier می‌تواند در پاسخ موجود باشد که در پیش‌تر توضیح داده شد.

بسیار مهم: ذخیره کردن اطلاعات توکن

بر روی user_name مقدار شماره موبایلی که احرازهویت با آن شکل گرفته قرار داده می‌شود.
متناظر با آن کاربر، مقادیر jti و access_token و expires_in و creation_time را باید ذخیره کنید.
هم‌چنین بهتر است مقادیر loa و scope را جهت بررسی عدم مغایرت با مقادیر اولیه درخواست خود مقایسه کنید.

به خاطر داشته باشید، آن چه از شما در زمان استعلامات قضایی و حقوقی خواسته می‌شود، مقدار شمارنده یکتا (jti) می‌باشد که باید مقدار access_token متناظر آن‌را برگردانید.
با توجه به اینکه عمر توکن‌ها محدود است و ممکن است در طول زمان یک کاربر(شماره موبایل) چندین توکن بگیرد، در صورت منقضی شدن توکن آن را از بانک اطلاعاتی حذف نکنید.

نمونه پاسخ خطا در صورت اشتباه بودن code (با status=403)

نمونه پاسخ خطا

```
{
  "status" : 403,
  "error_reason" : "کد وارد شده معتبر نمی‌باشد"
}
```

نمونه پاسخ خطا در صورت اشتباه بودن secure_code (با status=403)

نمونه پاسخ خطا

```
{
  "status" : 403,
  "error_reason" : "  مقدار کد امنیتی اشتباه است "
}
```

نمونه پاسخ خطا در صورت اشتباه بودن سرآیند Authorization (با status=401)

نمونه پاسخ خطا

```
{
  "status" : 401,
  "error_reason" : "اطلاعات هویت به درستی وارد نشده است"
}
```

نمونه پاسخ خطا در صورت اشتباه بودن redirect_uri (با status=400)

نمونه پاسخ خطا

```
{
  "status" : 400,
  "error_reason" : "مقدار آدرس بازگشتی اشتباه است"
}
```

سازمان فناوری اطلاعات ایران

صحت‌سنجی توکن

پس از پایان مرحله پنجم عملیات به پایان رسیده‌است ولی هنوز یک مسئولیت بر عهده کسب و کار وجود دارد و آن صحت‌سنجی توکن دریافت‌شده است.

هدف از این کار به وجود آوردن اطمینان برای کسب و کار است که توکن دریافت‌شده حتما از سامانه سماوا بوده است.

این صحت‌سنجی لازم است به ازای هر بار دریافت توکن انجام شود و در صورتی که قبل از انقضای توکن (با توجه به فیلد expires_in)، کاربر مجددا از توکن استفاده نماید نیازی به صحت‌سنجی مجدد نیست.

دو روش آنلاین و آفلاین برای صحت‌سنجی موجود است.

روش آنلاین (روش پیشنهادی)

سرویس صحت‌سنجی توکن

این سرویس بر روی آدرس پایه دریافتی از مقدار فیلد b2b_base_url در پاسخ مرحله اول قراردارد.

مقدار دریافت شده در مرحله اول طبق پاسخ دریافتی آن برابر با https://idtest.iran.ir می‌باشد که با توجه به آدرس خود این سرویس (یعنی /oauth/check_token) نمونه درخواست زیر با توجه به آن تولید شده‌است.

نمونه درخواست

نمونه درخواست صحت‌سنجی آنلاین توکن

```
POST /oauth/check_token HTTP/1.1
Host: idtest.iran.ir
Authorization: Basic dGVzdDpkNGE1NjBmYy1jNGMyLTExZWEtODdkMC0wMjQyYWMxMzAwMDM=
Content-Type: application/x-www-form-urlencoded

token=eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJjcmVhdGlvbl90aW1lIjoiMjAyMC0wNy0xNCAgMTE6NTI6NTcuNjI0IiwidXNlcl9uYW1lIjoiMDkxMjQ5NTg4MjAiLCJzY29wZSI6WyJtb2JpbGV
```

سازمان فناوری اطلاعات ایران

شرح سرآیند درخواست

نام سرآیند	مقدار	جنس
Authorization	• یک رشته ثابت با مقدار: اطلاعات رمز شده کسب و کار + کاراکتر فاصله + "Basic" ▪ **اطلاعات رمزشده کسب و کار**: در زمان ثبت نام، دو مقدار شناسه کلاینت (client_id) و رمز کلاینت (client_secret) به شما داده شده‌است. این دو رشته را به این ترتیب به هم‌دیگر الصاق کنید: **client_id:client_secret** (به کاراکتر : بین این دو دقت کنید) و سپس با روش Base64 کد کنید. به سرآیند Authorization در نمونه درخواست بالا دقت کنید.	رشته

شرح بدنه درخواست

نام فیلد	مقدار	جنس
token	توکن موردنظر	رشته

نمونه پاسخ(status=200)

نمونه پاسخ صحت‌سنجی توکن

```
{
    "active": true,
    "status": 200
}
```

سازمان فناوری اطلاعات ایران

شرح پاسخ(status=200)

نام فیلد	مقدار	جنس
active	true یا false	بولین (boolean)

۱. مقدارtrue : نشان‌دهنده‌ی معتبر بودن توکن است.

۲. مقدارfalse : نشان‌دهنده‌ی نامعتبر بودن توکن است.

نمونه پاسخ(status=401)

در صورتی که client_id یا client_secret به درستی وارد نشده باشد.

نمونه پاسخ خطا صحت‌سنجی توکن

```
{
  "status" : 401,
  "error_reason" : "اطلاعات هویت به درستی وارد نشده‌است"
}
```

نمونه پاسخ(status=400)

برای وقتی که توکن منقضی شده باشد.

نمونه پاسخ منقضی‌شدن توکن

```
{
    "active": false,
    "status": 400,
    "error_reason": "توکن منقضی شده‌است"
}
```

نمونه پاسخ(status=400)

برای وقتی که توکن معتبر نباشد.

نمونه پاسخ نامعتبر بودن توکن

```
{
    "active": false,
    "status": 400,
    "error_reason": "توکن منقضی شده‌است"
}
```

سازمان فناوری اطلاعات ایران

روش آفلاین

برای صحت‌سنجی نیاز به کلید عمومی سماوا می‌باشد. کسب و کار نیاز دارد در ابتدا شروع برنامه‌ی خود سرویس دریافت کلید عمومی را فراخوانی کرده و پس از آن به بازگشایی توکن‌های دریافتی بپردازد .
اما به دلیل آنکه، امکان دارد کلیدهای سامانه تغییر یابند روشی تعبیه شده که کسب و کار متوجه این تغییرشود و سرویس دریافت کلید عمومی را مجددا در طی این تغییر فراخوانی کرده و پس از دریافت کلید جدید اقدام به بازگشایی توکن‌های جدید نماید.
در پاسخ سرویس دریافت توکن در مرحله پنجم فیلدی در سرآیند پاسخ تحت عنوان kid قرار گرفته‌است که نشان‌دهنده‌ی شماره کلید مورد استفاده برای امضاء شدن توکن می‌باشد.

کسب و کار باید این مقدار (kid) را در سمت خود نگهداری‌کند و هربار که پاسخی از سرویس دریافت توکن در مرحله پنجم دریافت‌نمود آن را با مقدار فعلی نگهداشته شده مقایسه‌کند و در صورت مغایرت اقدام به فراخوانی سرویس دریافت کلید عمومی کند و توکن (JWT) جدید دریافت‌شده و توکن‌های پس از آن را با کلید عمومی جدید رمزگشایی کند.

سرویس دریافت کلید عمومی

این سرویس بر روی آدرس پایه دریافتی از مقدار فیلد b2b_base_url در پاسخ مرحله اول قراردارد.
مقدار دریافت شده در مرحله اول طبق پاسخ دریافتی آن برابر با https://idtest.iran.ir می‌باشد که با توجه به آدرس خود این سرویس (یعنی /oauth/token_key) نمونه درخواست زیر با توجه به آن تولید شده‌است.

نمونه درخواست

نمونه درخواست کلید عمومی

```
GET /oauth/token_key HTTP/1.1
Host: idtest.iran.ir
Authorization: Basic dGVzdDpkNGE1NjBmYy1jNGMyLTExZWEtODdkMC0wMjQyYWMxMzAwMDM=
```

شرح سرآیند درخواست

نام سرآیند	مقدار	جنس

نام سرآیند	مقدار	جنس
Authorization	یک رشته ثابت با مقدار: اطلاعات رمز شده کسب و کار + کاراکتر فاصله + "Basic" اطلاعات رمزشده کسب و کار: در زمان ثبت نام، دو مقدار شناسه کلاینت (client_id) و رمز کلاینت (client_secret) به شما داده شده‌است. این دو رشته را به این ترتیب به هم‌دیگر الصاق کنید: **client_id:client_secret** (به کاراکتر : بین این دو دقت کنید) و سپس با روش Base64 کد کنید. به سرآیند Authorization در نمونه درخواست بالا دقت کنید.	رشته

نمونه پاسخ(status=200)

نمونه پاسخ کلید عمومی

```
{
    "alg": "SHA256withRSA",
    "value": "-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzHPhTJKhXhoHjFd2K0HGgIPhwxidsFv
QbLtHxdQRKB/YJ+0OehyywYqwByM1q+7E0X2AB\n-----END PUBLIC KEY-----"
}
```

نمونه پاسخ کلید عمومی

```
{
    "alg": "SHA256withECDSA",
    "value": "-----BEGIN PUBLIC KEY-----
\nMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEBJRcLzeriul8Fy7KFLP9/WAyvOChNRTQbWrs9zq
d65CXRt9uxrTNWEWoI/dvzYbSSjGtnQBNbUvuVSZFKugtXQ==\n-----END PUBLIC KEY-----"
}
```

دلیل آنکه دو نمونه پاسخ قرارداده شده‌است آن است که سامانه سماوا از دو مدل کلید RSA و ECDSA پشتیبانی می‌کند و به همین دلیل فیلد alg می‌تواند مقدار متفاوتی داشته باشد.

سازمان فناوری اطلاعات ایران

شرح پاسخ

نام فیلد	مقدار	جنس
alg	الگوریتمی که نشان‌دهنده‌ی نحوه عملیات رمزنگاری مربوط به توکن تولیدشده می‌باشد.	رشته
value	کلید عمومی سامانه سماوا	رشته

نمونه پاسخ(status=401)

در حالتی که مقدار اطلاعات هویتی client_id یا client_secret اشتباه باشد.

نمونه پاسخ خطا کلیدعمومی

```
{
  "status" : 401,
  "error_reason" : "اطلاعات هویت به درستی وارد نشده‌است"
}
```

نحوه‌ی صحت‌سنجی توکن دریافتی در سمت کسب و کار

بهترین راه حل استفاده از کتابخانه‌های متن باز است که صحت توکن را با توجه به کلید عمومی بررسی می‌کنند.

هر زبانی دارای کتابخانه‌ای برای بازگشایی توکن JWT است.

بهترین کتابخانه‌ای که برای زبان‌های مبتنی بر JVM موجود است : io.jsonwebtoken. jjwt

نمونه کد در فایل فشرده **پیوست** با زبان Java قرار گرفته‌است.

سازمان فناوری اطلاعات ایران

لیست حوزه (scope)

نام	توضیح
mobile_number	به تمام کسب و کارها این حوزه پس از ثبت‌نام داده می‌شود و باعث می‌شود در توکن ساخته شده در فیلد user_name مقدار شماره موبایل شخص احراز شده قرار بگیرد.
national_number	بعضی از کسب و کارها نیاز دارند که کد ملی شخص احراز شده را نیز در توکن دریافت شده داشته‌باشند که باعث می‌شود فیلدی در سمت سرویس دریافت توکن (مرحله پنجم) اضافه شود به نام national_number که حاوی کد ملی شخص احراز شده‌است
person_identifier	به بعضی از کسب و کارها اجازه‌ی دریافت کد ملی داده نمی‌شود ولی نیاز دارند که یکتایی شخص را مورد بررسی قرار بدهند زیرا صرف شماره موبایل یکتایی را تضمین نمی‌کند (چون هر شخصی چندین شماره می‌تواند داشته باشد). با فرستادن این حوزه در مرحله اول باعث می‌شود سمت سرویس دریافت توکن (مرحله پنجم) فیلدی تحت عنوان person_identifier اضافه می‌شود که حاوی شناسه‌ی یکتایی است. در واقع کار یکتایی کد ملی را انجام می‌دهد ولی مقدارش چیز دیگری است.

سازمان فناوری اطلاعات ایران

خروجی سرویس‌ها در قالبPostman

از پیوست شماره ۲ می‌توانید خروجی فراخوانی سرویس‌ها را دریافت کنید.

در خروجی postman دقت شود که آدرس چهار سرویس برای فراخوانی موجود است.

۱. اولین سرویس به نام create oauth request که شامل درخواست مرحله اول سامانه می‌باشد.
۲. دومین سرویس به نام get-token که شامل فراخوانی سرویس دریافت توکن در مرحله ۵ می‌باشد.
۳. سومین سرویس به نام check-token که شامل سرویس صحت‌سنجی توکن می‌باشد.
۴. چهارمین سرویس به نام token_key که جهت دریافت کلید عمومی سامانه و صحت‌سنجی توکن‌ها به صورت آفلاین می‌باشد.

آدرس پایه سرویس‌های دو، سه و چهار به حالت داینامیک تبدیل شده که در پاسخ مرحله اول تحت عنوان b2b_base_url دریافت می‌شود.

سازمان فناوری اطلاعات ایران

قدم آخر

اگر ارتباط به سرور آزمایشی به خوبی صورت گرفت، با تأیید راهبر سامانه سماوا می‌توانید به سامانه اصلی متصل شوید.

کافی است کسب و کار آدرس پایه سرویس مرحله اول که بر روی https://idtest.iran.ir قرار گرفته بود را به https://idbtob.iran.ir تغییردهد.

بقیه سرویس‌ها به علت آنکه آدرس پایه آنها در پاسخ سرویس مرحله اول قرار گرفته شده‌است (b2b_base_url) نیازی به تغییر ندارند.