



سازمان امور مالیاتی کشور

## دفتر توسعه خوداظهاری و تمکین داوطلبانه

سد

«دستورالعمل فنی اتصال به سامانه مودیان»

شناسه سند:

RC\_TICS.IS\_v1.6

شهریور ۱۴۰۴

شناسه سند
RC_TICS.IS_v1.6
شهریور ۱۴۰۴

# سنده «دستورالعمل فنی اتصال به سامانه مودیان»



سازمان امور ملیان آنکوثر

## مقدمه

زیرسامانه‌ی جمع‌آوری صورتحساب یکی از زیرسامانه‌های سامانه‌ی مودیان است که وظیفه‌ی دریافت صورتحساب، ارسال به هسته، گرفتن نتیجه اعتبارسنجی صورتحساب و ذخیره کردن آن و پاسخ به استعلام‌های صورتحساب‌های ارسالی از سمت مودی را برعهده دارد. این زیرسامانه دارای یک وب‌سرویس می‌باشد که تمامی درخواست‌ها از طریق این وب‌سرویس به سامانه ارسال شده و پاسخ داده می‌شوند. این وب‌سرویس در چهار چوب REST API پیاده سازی شده و فراخوانی آن نیازمند احراز هویت<sup>۱</sup> مودی از طریق امضای دیجیتال می‌باشد.

در این سنده منابع موجود در این وب‌سرویس و نحوه فراخوانی و پاسخ دهی هر کدام شرح داده خواهد شد و در نهایت در قالب یک مثال فرآیند اتصال به سامانه مودیان و ارسال صورتحساب به طور کامل انجام می‌گیرد.

## ملاحظات

ردیف	عنوان
۱	این سنده، صورتحساب با الگوی پالایش و پخش را نیز پوشش می‌دهد.

<sup>۱</sup> Authentication

شناسه سند
RC_TICS.IS_v1.6
شهریور ۱۴۰۴

# سند «دستورالعمل فنی اتصال به سامانه مودیان»



## فهرست مطالب

۱ - تعاریف	۴
۲ - دریافت شناسه یکتای حافظه مالیاتی	۵
۳ - مراحل ارسال صورتحساب و استعلام وضعیت آن	۶
۴ - منابع در دسترس و کاربردهای هر کدام	۶
۵ - دریافت چالش تصادفی و احراز هویت	۹
۶ - دریافت اطلاعات سرور	۱۷
۷ - ارسال صورتحساب	۱۸
۸ - استعلام وضعیت صورتحساب‌های ارسالی	۳۳
۹ - استعلام اطلاعات حافظه و مودی	۴۲
۱۰ - استعلام وضعیت صورتحساب در کارپوشه	۴۴
۱۱ - ارسال پرداخت صورتحساب	۴۵
۱۲ - پیوست‌ها	۴۸

<p>شناسه سند RC_TICS.IS_v1.6</p> <p>شهریور ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	 <p>سازمان امور ملیان و کشور</p>
---	--	---

## ۱ - تعاریف

عنوان	تعریف
امضا دیجیتال <sup>۲</sup>	<p>فرآیندی که طی آن فرستنده پیام به وسیله‌ی یک کلید خصوصی، رشته‌ای به نام امضا تولید می‌کند و آن را در کنار اصل پیام برای گیرنده می‌فرستد. گیرنده با در اختیار داشتن کلید عمومی فرستنده می‌تواند نسبت به اصالت فرستنده اطمینان حاصل کند و مطمئن شود محتوای پیام در طول مسیر تغییری نکرده است.</p>
گواهی امضا <sup>۳</sup>	<p>گواهی الکترونیکی امضا برای اشخاص حقیقی یا گواهی الکترونیکی مهر سازمانی برای اشخاص حقوقی صادر شده توسط مراکز میانی صدور گواهی الکترونیکی، شامل کلید عمومی امضا، تاریخ انقضا و اطلاعات شناسایی هویتی افراد که در قالب یک فایل crt یا cer می‌باشد و برای بررسی صحت امضا بسته‌های ارسالی مورد استفاده قرار می‌گیرد.</p>
صورتحساب الکترونیک	<p>صورتحسابی است دارای شماره منحصر به فرد مالیاتی که اطلاعات مندرج در آن، در حافظه مالیاتی فروشنده ذخیره می‌شود. مشخصات و اقلام اطلاعاتی صورتحساب الکترونیکی، متناسب با نوع کسب و کار توسط سازمان تعیین و اعلام می‌شود. در مواردی که از دستگاه کارت‌خوان بانکی یا درگاه پرداخت الکترونیکی به عنوان پایانه فروشگاهی استفاده می‌شود، رسید یا گزارش الکترونیکی پرداخت خرید صادره در حکم صورتحساب الکترونیکی است.</p>
شماره مالیاتی	<p>شماره منحصر به فرد مشخص کننده یک صورتحساب شامل شناسه حافظه مالیاتی صادر کننده صورتحساب، تاریخ صدور، سریال صورتحساب و یک رقم کنترلی برای جلوگیری از صدور شماره مالیاتی‌های نامعتبر.</p>
شناسه یکتای حافظه مالیاتی	<p>شناسه‌ی یکتایی که توسط سازمان اختصاص یافته می‌شود و مودی می‌تواند از طریق کارپوشه آن را دریافت کند و از آن به منظور صدور صورتحساب استفاده می‌شود.</p>

Digital Signature<sup>۴</sup>

Digital Signature Certificate<sup>۵</sup>

شناسه سند RC_TICS.IS_v1.6	<b>سنده «دستورالعمل فنی اتصال به سامانه مودیان»</b>	 سازمان امور مالیاتی کشور
شهریور ۱۴۰۴		

## ۲ - دریافت شناسه یکتا حافظه مالیاتی

مودی جهت صدور و ارسال صورتحساب الکترونیکی نیاز به دریافت شناسه یکتا حافظه مالیاتی دارد.  
بنابراین می‌بایست به بخش عضویت و ثبت نام کارپوشه خود مراجعه نموده و مراحل زیر را طی نماید:

۱. به ازای هر شناسه یکتا حافظه مالیاتی، یکی از سه حالت ارسال اطلاعات صورتحساب را به شرح

ذیل انتخاب کند:

- توسط مودی

- توسط شرکت معتمد / سامانه های دولتی - با کلید مودی

- توسط شرکت معتمد / سامانه های دولتی - با کلید شرکت معتمد / سامانه های دولتی

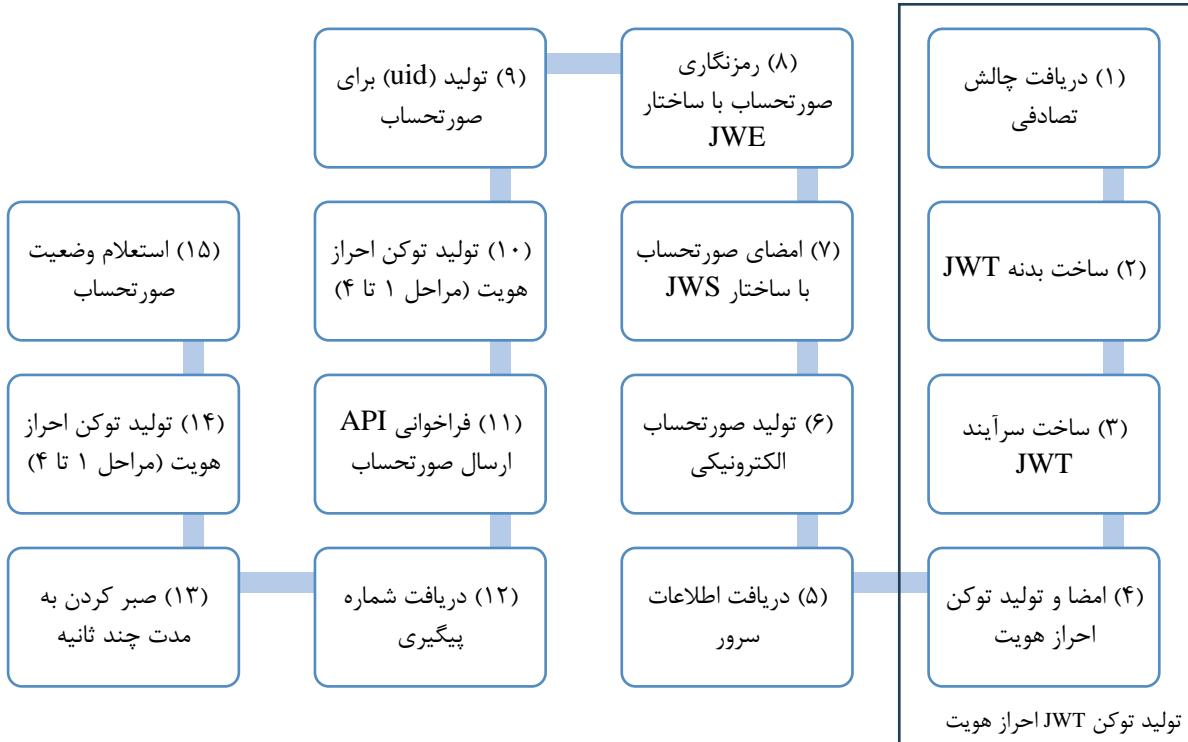
۲. کلید عمومی/گواهی امضاء دریافتی از مراکز میانی معتبر با طول کلید ۲۰۴۸ بیت را بارگذاری نماید. در این نسخه امکان بارگذاری گواهی امضاء نیز در کارپوشه افزوده شده است.

نکته: در صورتی که ارسال غیرمستقیم باشد و شرکت معتمد ارائه کننده خدمات مالیاتی صدور، رمزگذاری و ارسال صورتحساب را به عهده داشته باشد، بارگذاری کلید عمومی/گواهی امضاء توسط مودی ضرورتی ندارد. در این حالت شرکت معتمد ارائه کننده خدمات مالیاتی باید از طریق کارپوشه خود، کلید عمومی/گواهی امضاء مربوطه را به سازمان معرفی نماید.

**توجه:** این سند با هدف استفاده از نسخه دوم API‌های سامانه مودیان و جهت تسهیل در فرآیند ارسال صورتحساب و اتصال به سامانه مودیان منتشر شده است. در این نسخه قابلیت استفاده از گواهی امضاء برای احراز هویت و ارسال صورتحساب ایجاد شده است. لازم به ذکر است تا اطلاع ثانوی امکان استفاده از نسخه قبلی API‌های سامانه مودیان نیز فراهم می‌باشد که راهنمای استفاده از آن به پیوست این سند بارگذاری گردیده است.

<p>شناسه سند RC_TICS.IS_v1.6</p> <p>شهریور ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	 <p>سازمان امور مالیاتی کشور</p>
---	--	---

## ۳ - مراحل ارسال صورتحساب و استعلام وضعیت آن



## ۴ - منابع در دسترس و کاربردهای هر کدام

وب سرویس جمع‌آوری سامانه‌ی مودیان در آدرس <https://tp.tax.gov.ir/requestsmanager> در دسترس می‌باشد. منابع موجود در این وب سرویس شامل موارد زیر است (جدول ۱) که توضیحات کامل هر کدام به همراه مثال در ادامه به شکل کامل داده خواهد شد فراغوایی همه‌ی منابع موجود در وب‌سرویس جمع‌آوری سامانه‌ی مودیان نیازمند احراز هویت فراغوایی کننده می‌باشند. به جز منبع دریافت چالش تصادفی که به منظور احراز هویت به کار می‌رود که جزئیات آن در ادامه توضیح داده خواهد شد.

توضیحات	ساختار خروجی	درخواست	آدرس
دريافت چالش تصادفي <a href="#">راهنما در صفحه ۱۰</a>	{     "nonce": "string",     "expDate": "string" }	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/nonce?timeToLive=20' \ -H 'accept: */*'</pre>	GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/nonce">https://tp.tax.gov.ir/requestsmanager/api/v2/nonce</a>
ارسال صورتحساب <a href="#">راهنما در صفحه ۱۸</a>	{     "timestamp": 0,     "result": [         {             "uid": "string",             "packetType": "string",             "referenceNumber": "string",             "data": "string"         }     ] }	<pre>curl -X 'POST' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/invoice' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGci [ JWT Token ] dLcdPeI_9Q' \ -H 'Content-Type: application/json' \ -d '[' {     "payload": "eyJhbGciOiJ...[ JWE ]...EEzZe9mxIxw",     "header": {         "requestTraceId": "cf019c26-f235-11ed-a05b-0242ac120003",         "fiscalId": "A11216"     } } ]'</pre>	POST <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/invoice">https://tp.tax.gov.ir/requestsmanager/api/v2/invoice</a>
دريافت اطلاعات پرونده‌ی مودی <a href="#">راهنما در صفحه ۴۳</a>	{     "nameTrade": "string",     "taxpayerStatus": "string",     "nationalId": "string" }	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer?economicCode=14003778990' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbG...[ JWT Token ]...klQXOuA'</pre>	GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer">https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer</a>
دريافت اطلاعات حافظه <a href="#">راهنما در صفحه ۴۲</a>	{     "nameTrade": "string",     "fiscalStatus": "string",     "nationalId": "string",     "economicCode": "string" }	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information?memoryId=A11216' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGc...[ JWT Token ]...OFh9zw'</pre>	GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information">https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information</a>
دريافت اطلاعات سرور <a href="#">راهنما در صفحه ۱۷</a>	{     "serverTime": 0,     "publicKeys": [         {             "key": "string",             "id": "string",             "algorithm": "string",             "purpose": 0         }     ] }	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/server-information' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGci...[JWT]...Jv18fvHm0PKVA'</pre>	GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/server-information">https://tp.tax.gov.ir/requestsmanager/api/v2/server-information</a>

<p>استعلام صورتحساب با شماره پیگیری <u>۳۴ راهنمای صفحه</u></p>	<pre>[   {     "referenceNumber": "string",     "uid": "string",     "status": "string",     "data": {},     "packetType": "string",     "fiscalId": "string",     "sign": "string"   } ]</pre>	<pre>curl -X 'GET' \   'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by- reference-id?referenceIds=f9173085-2316-4ca6-918e- e41aaf7ef8dd&amp;referenceIds=93367b02-23dd-4568-90e1- 2b47d799f361&amp;start=2023-05- 14T10%3A00%3A00.00000000%2B03%3A30&amp;end=2023-05- 14T21%3A00%3A00.00000000%2B03%3A30' \   -H 'accept: */*' \   -H 'Authorization: Bearer eyJhbGc...[ JWT TOKEN ]...q4RcXogA'</pre>	<p>GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-reference-id">https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-reference-id</a></p>
<p>استعلام با شناسه درخواست (uid) <u>۳۷ راهنمای صفحه</u></p>	<pre>[   {     "referenceNumber": "string",     "uid": "string",     "status": "string",     "data": {},     "packetType": "string",     "fiscalId": "string",     "sign": "string"   } ]</pre>	<pre>curl -X 'GET' \   'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by- uid?uidList=cb080c58-e36f-4bb0-a932- 90f672109fb6&amp;uidList=b3bd6327-1c57-4cae-85ed- 5c88de28aea3&amp;fiscalId=A111YO&amp;start=2023-06- 10T00%3A00%3A00.00000000%2B03%3A30&amp;end=2023-06- 10T23%3A59%3A59.99999999%2B03%3A30' \   -H 'accept: */*' \   -H 'Authorization: Bearer eyJhbGciO...[ JWT TOKEN ]...ski8e-A'</pre>	<p>GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-uid">https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-uid</a></p>
<p>استعلام براساس بازه زمانی <u>۴۰ راهنمای صفحه</u></p>	<pre>[   {     "referenceNumber": "string",     "uid": "string",     "status": "string",     "data": {},     "packetType": "string",     "fiscalId": "string",     "sign": "string"   } ]</pre>	<pre>curl -X 'GET' \   'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry?start=202 3-06-10T00%3A00%3A00.00000000%2B03%3A30&amp;end=2023-06- 10T23%3A59%3A59.99999999%2B03%3A30&amp;pageNumber=1&amp;pageSize=10' \   -H 'accept: */*' \   -H 'Authorization: Bearer eyJhbGci...[ JWT TOKEN ]...KXzBjRZw'</pre>	<p>GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry">https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry</a></p>

جدول ۱

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امور ملیان گلوبال</p>
---	---	---------------------------------

## - ۵ - دریافت چالش تصادفی و احراز هویت

مکانیزم احراز هویت در وبسرویس جمع‌آوری سامانه‌ی مودیان بر اساس استاندارد «پروتکل احراز هویت در زیرساخت کلید عمومی ایران» منتشر شده توسط «مرکز دولتی صدور گواهی الکترونیک ریشه» می‌باشد که بر مبنای امضای دیجیتال طراحی شده. جهت اتصال به این وب سرویس و پیاده‌سازی این پروتکل لازم است که یک امضای دیجیتال شامل کلید خصوصی امضاء یا توکن امنیتی، به همراه گواهی امضای الکترونیک معتبر، صادر شده توسط مراکز صدور گواهی الکترونیک میانی - در اختیار داشته باشد.

### - ۱ - مراحل احراز هویت هر درخواست

مراحل احراز هویت درخواست به شکل زیر است که در ادامه جزئیات هر یک شرح داده می‌شود:

۱. دریافت چالش تصادفی<sup>۴</sup> (رشته‌ی تصادفی)
۲. قرار دادن clientId و nonce و ساختن payload توکن JWT
۳. ایجاد header توکن JWT براساس ساختار مشخص و قراردادن گواهی امضا در آن
۴. امضای header و payload براساس استاندارد JWS و ساخت توکن
۵. فرخوانی درخواست بعدی با قرار دادن توکن در سرآیند درخواست

فرآیند احراز هویت بدین صورت است که ابتدا شما باید API چالش تصادفی را فرخوانی کنید. این API نیاز به اعتبارسنجی ندارد و یک رشته تصادفی یکبار مصرف و دارای مهلت استفاده محدود تولید کرده و به شما می‌دهد. شما باید قبل از منقضی شدن این رشته آن را به همراه گواهی امضای خود امضا کرده و در درخواست بعدی در بخش Http Header به عنوان توکن ارسال نمایید.

توجه شود که فرآیند گرفتن Nonce و تولید توکن، برای انجام هر درخواست الزامی است و توکنی که برای یک درخواست ساخته می‌شود تنها یکبار قابل استفاده خواهد بود.

---

<sup>۴</sup>Nonce

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امور ملی اینترنت</p>
---	---	--------------------------------

## ۵-۱-۱-۱ دریافت چالش تصادفی

این API یک ورودی timeToLive دارد که زمان اعتبار چالش تصادفی را مشخص می‌کند. در صورتی که این ورودی خالی باشد به طور پیشفرض چالش ۳۰ ثانیه معتبر خواهد بود. در پاسخ رشته تصادفی تولید شده برگردانده می‌شود.

Get Nonce - چالش تصادفی	
آدرس	Method
<a href="https://tp.tax.gov.ir/requestsmanager/api/v2/nonce">https://tp.tax.gov.ir/requestsmanager/api/v2/nonce</a>	GET
<ul style="list-style-type: none"> <li>▪ timeToLive: مدت زمان اعتبار رشته تصادفی به ثانیه</li> <li>○ نوع ورودی: اختیاری</li> <li>○ محل قرارگیری: Request Params</li> <li>○ مقدار پیشفرض: ۳۰</li> <li>○ مقادیر مجاز: ۱۰ تا ۲۰۰</li> </ul>	ورودی
<ul style="list-style-type: none"> <li>▪ nonce: رشته تصادفی تولید شده</li> <li>▪ expDate: زمان انقضای رشته تصادفی</li> </ul>	خروجی

نمونه درخواست دریافت چالش تصادفی:

```
curl -X 'GET' \
'https://tp.tax.gov.ir/requestsmanager/api/v2/nonce?timeToLive=20' \
-H 'accept: */*'
```

خروجی برابر است با:

```
{
  "nonce": "ab202a55-e106-445c-b2a3-5a7364991a66",
  "expDate": "2023-08-22T16:07:18.277824208Z"
}
```

## ۵-۱-۲-۱ امضای Nonce و تولید توکن

پس از دریافت رشته تصادفی Nonce، این رشته باید تبدیل به توکن JWS شود و امضا شود. فرمت توکن JWS تولید شده به شکل زیر است:

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	<p>سازمان امور ملی ایمنی و کنترل</p>
---	--	--------------------------------------

### ساختار توکن JWS

یک شیء JSON دارای فیلدهای زیر:

- alg: الگوریتم امضا: RS256

x5c: لیستی که شامل گواهی امضای مودی باشد. کد شده به فرمت Base64

- sigT: زمان امضای توکن

فرمت:

YYYY-MM-dd'T'HH:mm:ss'Z'

نمونه:

2023-05-13T10:44:47Z

"sigT": لیستی از فیلدهای ضروری در قسمت Header. تنها شامل رشته‌ی "crit"

توجه کنید که مقدار فیلد sigT باید طبق استاندارد ISO\_8601 باشد و در صورتی که با کاراکتر Z ختم شود باید به منطقه زمانی UTC باشد. در صورتی که بخواهید زمان محلی را در امضای صورتحساب ارسال نمایید می‌توانید در انتهای آن عبارت "+0330" را اضافه کنید:

2023-05-13T14:14:47Z+0330

همچنین در فیلد x5c که به صورت لیست است، می‌توانید گواهی امضای مرکز میانی صادرکننده‌ی گواهی خود را نیز ارسال نمایید که به عنوان زنجیره گواهی‌های تایید کننده‌ی بسته شناخته می‌شوند تا به یک گواهی مورد اعتماد برسد (Trusted cert). البته این مورد ضرورتی ندارد زیرا گواهی‌های معتبر تمامی مراکز میانی فعال و گواهی مرکز ریشه همگی به عنوان گواهی‌های مورد اعتماد شناخته می‌شوند.

**Header**

یک شیء Json دارای دو فیلد زیر:

- nonce: رشته تصادفی یکبار مصرف دریافت شده

- clientId: شناسه ارسال کننده صورتحساب

**Payload**

برای مودیان همان شناسه حافظه صادر کننده صورتحساب

برای شرکت‌های معتمد شناسه شرکت معتمد

ورودی الگوریتم امضا برابر است با:

ASCII (BASE64URL (UTF8 (JWS Protected Header)) ) || . . . || BASE64URL (JWS Payload))

**Signature**

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	<p>سازمان امور ملیان گوشه‌ر</p>
---	--	---------------------------------

الگوریتم مورد استفاده در امضای توکن، RSASSA-PKCS1-v1\_5 using SHA-256 است و می‌باشد.

کلید خصوصی امضا باید کلید خصوصی معادل با گواهی فرستاده شده در بخش header باشد که امضای توکن توسط آن گواهی Verify شود.

مطابق استاندارد RFC7515 قالب چیدمان توکن JWS به صورت زیر است:

```
BASE64URL (UTF8 (JWS Protected Header)) ||| '.' ||
BASE64URL (UTF8 (JWS Payload)) ||| '.' ||
BASE64URL (JWS Signature)
```

توجه کنید که فرمت Header بسته‌ی JWS و محتويات بسته (Payload) باید حتما utf-8 باشد و رشته‌ی Header و Payload برای امضا و تولید توکن به فرمت Base64URL کد می‌شود. برای اطلاعات بیشتر سند RFC7515 را مشاهده کنید: <https://www.rfc-editor.org/rfc/rfc7515>

لازم به ذکر است گواهی استفاده شده در فرآیند امضای توکن احراز هویت می‌باشد معتبر بوده و کد ملی/شناسه ملی موجود در گواهی<sup>۵</sup> با مشخصات ارسال کننده درخواست (صاحب clientId) منطبق باشد.

بعنوان مثال فرض کنید Header توکن ما یک Json به شکل زیر باشد:

```
{"crit":["sigT"], "sigT": "2024-03-06T13:05:50Z", "x5c": ["MIIDejCCAmKgAwIBAgIUV27QXqJjK2EgFy9zeYkpsX+ISPswDQYJKoZIhvcNAQELBQAwcTELMAkGA1UEBhMCSVIXDDAKBgNVBAgMA1RlaDEMMAoGA1UEBwwDVGVoMREwDwYDVQQKDAhNb2hheW1lbjEMMAoGA1UECwwDVGf4MSUwIwYJKoZIhvcNAQkBFhZtLm1hbHZlcmRpQG1vaGF5bWVuLmlybMB4XDTIzMDMyNDEzMjgyM1oXDTI0MDMyMzEzMjgyM1owTTEPMA0GA1UEAwwGQW56YWxpMRcwFQYDVQQKDA5RdW9WYWRpcyBhcm91cDELMAkGA1UEBhMCSVIXFDASBgNVBAUTCzE0MDAzNzc4OTkwMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEazLgyk5KO6+j9d1ud0i1JArrZ3Whw/w9wEzHB9yXwENRa5fm5AbRukMF5b6VGeKzD6LZuL9+tfdfFfWyPcjI++gGNy wzRmEHKpTnzP1t6NyuxKfm4nBVAb1sugSw8Y5DEXRFTqILgBWN/pZ4zGlifEALMcGAs7ADcjnv7b/tM2wxr9rHxsCvW4HvlzQasK8QrlCrKgt0E166rSXCHep/uIONDwp0W2Oe1M1zTm6AAjWXRLGcshPIHuK+ZLfaFxWtoGonf6qn9ypos2B18D/EFa8WHON62eYKT0kW3jBVa3yPEkRwdDjDu/3CPz ymh f3WFYwxpb4t35oWb/qUXGVIdvwIDAQABoy4wLDAfBgNVHSMEGDAwqBSx+Oq+RO3x/FmyCp+jcmf OH+Fn9TAJBgNVHRMEAjaAMA0GCSqGSIb3DQEBCwUA4IBAQAgKATXlnS+pPtAiRIYGtydVU5Vi7Aq+D6QW07uFqcb7vBhddN3yX21VVcwpTNJzhv8UCM+mDMv1msRVKvtMoo5fhfII92/Wo8rUz1RP+yhyCk0Vz8I11v+bjLwVur/agC/s5Rf0m66pNNjFZ9J3S2N31ChXYwz2vvA8pdAYvWTu9g5u4FMFqlsaLwMGC+WaA0g3KYzRkdWRy1vd23hLTucVsWM8wpgZ11wEGE1khca/Sd0mCU2HG5vIbqFFtjA6to0fY07CE5fD8aR3UcXjNduosVO52ZqCX5SabrhFS3AGHFRjpFnI5LZespicCXSA8Sv3kOSCSRQKqFbiwSFM8Zjg"], "alg": "RS256"}
```

همچنین Payload درخواست ما به فرمت utf-8 شیء زیر است:

<sup>5</sup> فیلد SUBJECT در قسمت SERIALNUMBER گواهی امضاء

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	<p>سازمان امور ملیا بنگلور</p>
--	--	--------------------------------

```
{
  "nonce": "91dc28af-4c95-47f0-9913-87f8162b1708-1709717749862",
  "clientId": "A11226"
}
```

با امضای رشته با الگوریتم RS256 و الصاق امضای تولید شده به رشته اصلی (به وسیله‌ی یک ".")،

توکن JWT ساخته می‌شود:

eyJjcmI0IjpbInNpz1QiXSwic2lnVCI6IjIwMjQtMDMtMDZUMTM6MDU6NTBaIiwieDVjIjpbIk1JSUR1akNDQW1Lz0F3SUJBZ01VVjI3UVhxSmpLMkVnRnk5emVza3BzWctJU1Bzd0RRWUpLb1pJaHZjTkFRRUxCUUF3Y1RFTE1Ba0dBMVVFQmhNQ1NWSXhEREFLQmdOVkJBZ01BMVJsYURFTU1Bb0dBMVVFQnd3RFZHVm9NUkv3RHdZRFZRUUTEQWhOYjJoaGVXMWxiakVNTUFvR0ExVUVDd3dEVkdGNE1TVxdJd1lKS29aSh2Y05BUwtCRmhadExtMWhiSFpsY21ScFFHMXZhR0Y1Y1dWdUxtbH1NQjRYRFRJek1ETX1OREV6TWpneU0xb1hEVEkwTURNeU16RXpNamd5TTFvd1RURVBNTQTBHQTFVRUF3d0dRVzU2WVd4cE1SY3dGUv1EV1FRS0RBNVJkVz1XWVdScGN5QkhjbTkxY0RFTE1Ba0dBMVVFQmhNQ1NWSXhGREFTQmdOVkJBVVRDekUwTURBek56YzRPVgt3TU1JQk1qQU5CZ2txaGtpRzl3MEJBuuVGQUFPQ0FROEFNSU1CQ2dLQ0FRRUF6TGd5azVLTzYraj1kMXVkmG1sSkFyclozV2h3L3c5d0V6SEI5eVh3RU5SYTVmbTVBY1J1a01GNWI2Vkd1S3pENkxadUw5K3RmZEzmV31QY2pJKytnR055d3pSbUVIS3BUBnpQMXQ2Tn11WetmbTRuQ1ZBYmxzdWdTdzHZNURFWFJmVHFJTGdCV04vcFo0ekdsaWZFQuXNY0dBczdBRGNqbnY3Yi90TTJ3eHI5ckh4c0N2VzRIdmx6UWFzSzhRcjFDcktnVDBFSTY2c1NYQ0h1cC91SU9ORFdwmFCyt2VsTwadE02QUFqV1hSTEdjC2hQSUh1SytaTGZBRnhXdG9Hb25mNnFOOX1wb3MyQje4RC9FRmE4V0hPTjYyZV1LVDBrVzNqQ1ZhM31QRwtSd2tkRGpEds8zQ1B6eW1oZjNXR113eHBiNHQzNW9XYi9xVVhHVk1kdndJREFRQUJveTR3TERBZkJnT1ZIU01FR0RBV2dCU3grT3ErUk8zeC9GbX1DcCtqY21mT0grRm45VEFKQmdOVkhSTUVBakFBTUEwR0NTcUdTSWIzRFFFQkN3VUFBNE1CQVFBZ0tBVFhsb1MrcFB0QW1SSV1Hd1kV1U1Vm3QXErRDZRVzA3dUzxY0I3dkJzGROM31YMMxWVmN3cFROSnpodjhVQ00rbURNdmxtc1JWS1Z0TW9vnNWZ1Zk1JOTIVv284c1V6MVJQK31oeUNrMFZ6OEkxMXYrYmpMd1Z1ci9hz0MvczVSzjBtNjZwTk5qRlo5SjNTMk4zbENoWF13ejJ2dkE4cGRBWZXXVHU5ZzV1NEZNrnFsc2FMd01HQytXYUEwZzNLWXpSa2RXUnkxdmQyM2hMVFVjVnNXTTh3cGdaMTF3RUDFMWt0y2EvU2QwbUNVMkhHNXZJYnFGZ1RqQTZ0bzBmWTA3Q0U1ZkQ4YVIzVWNYak5kdW9zV81M1pxQ1g1U2FicmhGUzNBR0hGUmpwRm5JNUxaZXNwaUNYU0E4U3Yza09TQ1NSUUTxRmJpd1NGTThaamciXswiYWxnIjoiUlMyNTYifQ.ew0KICAibm9uY2UiOiaiOTFkYzI4YWYtNGM5NS00N2YwLTk5MTMtODdmODE2MmIxNzA4LTE3MDk3MTc3NDk4NjIiLA0KICAIY2xpZW50SWQiOiaiQTEXMjI2Ig0KfQ.qPsK\_S-76JrYRerFsb18SqVSNQTCuAd1o496mE\_5Xof-bw1BgLd3bC33Vxrfqs0lpxSm5hyiKpMYkaz-GPWxt9meoHozRN1FAGimWuke26pH7VJD4vJqfWN784k82XwHRLv1UVoPkzfmtRiFYTwI2hGc1B7AfY\_I6cP5uGMBOY3Kqok0hh1fQyBM\_EIoSRNSW3JBAzHQea-EIm55oXkvXo\_2lwsmGHXngFA6qhDbzuHJ2mkItor2HJjZTbND9sxN-X1ZgSuM7i6izvxxTuSaQMWAfTrEv9d2BzG1ZT1zcFBZVXLaza13Bh74P5DhWsoOR8q0EJvgMvbKnWaX-H-c\_A

تکه کد زیر به زبان جاوا اعمالیات ساخت توکن از روی Nonce را انجام می‌دهد. لازم به ذکر است تمامی

این فرآیندها در کیت توسعه نرم افزاری جاوا و net. پیاده‌سازی شده‌اند و این تکه کد صرفاً جهت آشنایی بهتر با فرآیند تولید توکن JWT قرار داده شده است. همچنین کلید خصوصی‌ای که فرآیند امضا با آن انجام شده در

قسمت پیوست قرار گرفته است:

```
/** Loading Signature Private Key in PKCS#8 format */
String privateKeyPath = "path/to/private-key.pem";
KeyFactory keyFactory = KeyFactory.getInstance("RSA");
final PEMParser pemParser = new PEMParser(new FileReader(privateKeyPath));
final PrivateKeyInfo pemKeyPair = (PrivateKeyInfo) pemParser.readObject();
```

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	<p>سازمان امور ملیان گلزار</p>
--	--	--------------------------------

```

final byte[] encoded = pemKeyPair.getEncoded();
PrivateKey privateKey = keyFactory.generatePrivate(new
PKCS8EncodedKeySpec(encoded));

/** Loading Certificate */
String certificatePath = "path/to/certificate.crt";
CertificateFactory certificateFactory =
CertificateFactory.getInstance("X.509");
X509Certificate certificate = (X509Certificate)
certificateFactory.generateCertificate(new
FileInputStream(certificatePath));

/** Generate Signature Time */
String dateFormat = "yyyy-MM-dd'T'HH:mm:ss'Z'";
DateTimeFormatter dateTimeFormatter =
DateTimeFormatter.ofPattern(dateFormat, Locale.ROOT);
String signatureTime =
LocalDateTime.now(ZoneOffset.UTC).format(dateTimeFormatter);

String payload = "{\"nonce\": \"91dc28af-4c95-47f0-9913-87f8162b1708-
1709717749862\", \"clientId\": \"A11226\"}";

/** Generating JWT */
final JsonWebSignature jws = new JsonWebSignature();

jws.setPayload(payload);
jws.setAlgorithmHeaderValue(AlgorithmIdentifiers.RSA_USING_SHA256);
jws.setKey(privateKey);
jws.setCertificateChainHeaderValue(certificate);
jws.setHeader("sigT", signatureTime);
jws.setHeader("crit", new String[]{"sigT"});

jws.sign();

String jwt = jws.getCompactSerialization();

```

در ابتدا کلید خصوصی امضا به فرمت PKCS#8 در شیء privateKey بازگذاری می‌شود. سپس گواهی امضای مودی در قالب یک شیء از نوع X509Certificate باز می‌شود. سپس تاریخ امضا به فرمت مشخص شده تولید می‌شود. در نهایت با ساخت header درخواست و قراردادن آن در کنار payload داده شده و با در اختیار قرار داشتن کلید خصوصی امضا، توکن jwt ساخته می‌شود. جهت امضای رشته و تولید jwt در این تکه کد از کتابخانه‌ی jose-4j نسخه‌ی ۰.۹.۳ استفاده شده است. همچنین تکه کد زیر به زبان .NET. همین عملیات را انجام می‌دهد:

```

namespace TaxCollectData.Sample;
using System.Globalization;
using System.Text.Json;
using System.Text.Json.Nodes;
using JWT.Algorithms;
using JWT.Builder;

```

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امور ملیان گلزار</p>
--	---	--------------------------------

```

using Org.BouncyCastle.Crypto.Parameters;
using Org.BouncyCastle.OpenSsl;
using Org.BouncyCastle.Security;

internal class SignTest
{
    public static void Main(string[] args)
    {
        // Loading Signature Private Key in PKCS#8 format
        var privateKeyPemReader = new
        PemReader(File.OpenText("path/to/private-key.pem"));
        var privateKey = DotNetUtilities.ToRSA((RsaPrivateCrtKeyParameters)
privateKeyPemReader.ReadObject());

        // Loading Certificate
        var certPemReader = new PemReader(new
        StreamReader("path/to/certificate.crt"));
        var certificate =
        DotNetUtilities.ToX509Certificate((Org.BouncyCastle.X509.X509Certificate)
certPemReader.ReadObject());
        var publicKey = DotNetUtilities.ToRSA((RsaKeyParameters)
DotNetUtilities.FromX509Certificate(certificate).GetPublicKey());

        var payload = "{\"nonce\": \"91dc28af-4c95-47f0-9913-87f8162b1708-
1709717749862\", \"clientId\": \"A11226\"}";

        // Generating JWT
        var jws = JwtBuilder.Create()
            .WithAlgorithm(new RS256Algorithm(publicKey, privateKey))
            .AddHeader(HeaderName.X5C, new[]
{Convert.ToString(certificate.GetRawCertData())})
            .AddHeader("sigT", DateTime.UtcNow.ToString("yyyy-MM-
dd'T'HH:mm:ss'Z'", CultureInfo.InvariantCulture))
            .AddHeader("crit", new[] {"sigT"})
            .Encode(JsonSerializer.Deserialize<JsonNode>(payload));

        Console.WriteLine(jws);
    }
}

```

این کد از پکیج های زیر برای امضای بسته استفاده می نماید:

```

<PackageReference Include="jose-jwt" Version="4.1.0" />
<PackageReference Include="JWT" Version="10.0.2" />
<PackageReference Include="System.Security.Cryptography.Cng"
Version="6.0.0-preview.4.21253.7" />
<PackageReference Include="System.Security.Cryptography.X509Certificates"
Version="4.3.2" />
<PackageReference Include="Portable.BouncyCastle" Version="1.9.0" />

```

### ۵-۱-۳ - استفاده از توکن تولید شده در درخواست بعدی

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	<p>سازمان امور ملی اینترنت</p>
---	--	--------------------------------

حال باید با استفاده از این توکن هنگام ارائه‌ی درخواست بعدی خود را به سرور معرفی نمائیم. بدین منظور باید در سرآینده درخواست HTTP ارسالی، فیلد Authorization را برابر با "Bearer [token]" قرار دهیم. مثلا فرض کنید می‌خواهیم درخواستی برای گرفتن اطلاعات سرور انجام دهیم. این API از طریق <https://tp.tax.gov.ir/requestsmanager/api/v2/server-information> در دسترس است.

```
curl --location 'https://tp.tax.gov.ir/requestsmanager/api/v2/server-information' --header 'Authorization: Bearer eyJhbGciO....'
```

در صورتی که در Authorization مقدار توکن به درستی وارد شده باشد، امضای توکن صحیح باشد، گواهی امضا معتبر باشد،Nonce هنوز معتبر باشد و تاکنون استفاده نشده باشد، پاسخ به درخواست به شکل زیر خواهد بود:

```
{
  "serverTime": 1683985068801,
  "publicKeys": [
    {
      "key": "MIICIJANBgkq...",
      "id": "6a2bcd88-a871-4245-a393-2843eafe6e02",
      "algorithm": "RSA",
      "purpose": 1
    }
  ]
}
```

بررسی امضای توکن JWS بدین صورت است که هر یک از شرایط زیر برای صحت امضای بسته بررسی می‌شوند و در صورت وجود خطأ در هر بخش صحت امضای بسته زیر سوال می‌رود و توکن فرستاده شده مورد قبول واقع نمی‌شود:

۱. ساختار کلی بسته‌ی JWS (payload و header و signature) ارسال شده صحیح باشد.
۲. امضای موجود در بسته‌ی JWS با گواهی امضای فرستاده شده در قسمت header توکن ارسالی Verify شود.

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	 <p>سازمان امور ملیان آنکوثر</p>
---	---	---

۳. گواهی امضای فرستاده شده در header توسط یکی از مراکز میانی مورد اعتماد زیرسامانه‌ی جمع‌آوری صادر شده باشد و امضای گواهی با یکی از گواهی‌های موجود در مخزن Trusted Cert اعتبارسنجی و Verify شود.

۴. تاریخ انقضای گواهی امضا سپری نشده باشد.

۵. در صورت وجود فیلد CRL Distribution Point در فیلد‌های موجود در گواهی (قسمت Extension) استعلام لیست گواهی‌های ابطال شده پیش از موعد از مرکز میانی مورد نظر گرفته می‌شود و بررسی می‌شود گواهی مورد نظر جزو گواهی‌های ابطال شده‌ی پیش از موعد نباشد.

۶. در صورت وجود فیلد Authority Information Access در فیلد‌های موجود در گواهی (قسمت Extension) و وجود Access Method برابر با OCSP، از آدرس OCSP موجود در گواهی که آدرس سرور OCSP مرکز میانی صادر کننده‌ی گواهی می‌باشد، وضعیت گواهی استعلام گرفته می‌شود که گواهی دچار ابطال پیش از موعد نشده باشد.

## ۶ - دریافت اطلاعات سرور

این وب‌سرویس اطلاعات سرور مانند timestamp و کلیدهای عمومی رمزگذاری سامانه مودیان را بر می‌گرداند. همانطور که گفته شد فرآخوانی این API نیاز به احراز هویت دارد و جهت فرآخوانی آن باید توکن JWT در قسمت درخواست در فیلد Authorization فرستاده شود. نحوه کار این API به صورت زیر است:

دریافت اطلاعات سرور - Get server-information	
https://tp.tax.gov.ir/requestsmanager/api/v2/server-information	آدرس
GET	Method
ندارد	ورودی
شیء Json دارای فیلد‌های زیر: serverTime: برچسب زمانی سرور publicKeys: آرایه Json از کلیدهای عمومی رمزگذاری سرور هر یک شامل:	خروجی

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سنده دستورالعمل فنی اتصال به سامانه مودیان</b></p>	<p>سازمان امور ملی اینترنت</p>
---	--	--------------------------------

key: کلید کد شده به فرمت Base64 ○

id: شناسه کلید ○

algorithm: فعلاً برابر با "RSA" ○

purpose: مقدار ثابت ۱ ○

نمونه درخواست ارسالی و پاسخ آن:

```
curl -X 'GET' \
  'https://tp.tax.gov.ir/requestsmanager/api/v2/server-information' \
-H 'accept: */*' \
-H 'Authorization: Bearer eyJhbGciOi...[JWT]...Jv18fvHmOPKVA'
```

در صورت صحت توکن و درست بودن ساختار درخواست خروجی برابر است با:

```
{
  "serverTime": 1684055518885,
  "publicKeys": [
    {
      "key": "MIICIJANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAGEAxdzREOEfk3vBQogDPGTMqdDQ7t0oDhuKMZkA+Wm1hzjjhAGfSUOUdVOKRoUEQwP8oUcXRmYzcvCUGcfORT5iz7HbovqH+bIeJwT4rmLmFcgbPke+E3DLUxOtIZifEXrKXWgSVPkRnhMgym6UiAtnzwA1rmKstJoWpk9Nv34CYgTk8DKQN5jQJqb9L/Ng0zOEETi3zA424tsd9zv/kP4/SaSnbbnj0evqsZ29X6aBypvnTnwH9t3gbWM4I9eAVQhPYClawHTqvadaz/O/feqfm06QBFnCgL+CBdjLs30xQSLsPICjn1V1jMzoTZnAabWP6FRzzj6C2sxw9a/WwlXrKn3gldz7Ctv6Jso72cEeCeUI1tzHMDJPU3Qy12RQzaXujpMhCz1DVa47RvqiumpTNyK9HfFIIdhgoupFkxt14XLD165S55MF6HuQvo/RHSbBJ93FQ+2/x/Q2MNGB3BXOjNwM2pj3ojbDv3pj9CHzvayQUYM1y0cFmIJqj72uvVf9Jx9iTobaNNF6p152ADmh85GTAH1hz+4pR/E9IAxUI1/YiUneYu0G4tiDY4ZXykJYNknNfhSgxmngPHT+7kL31nyxgjiEEhK0B0vagWvdRCNJSNGwpLtlq4FLCWTAnPI5ctiFgq925e+sySjNaORCoHraBXNEwyiHT2hu5ZipIW2cCAwEAAQ==",
      "id": "6a2bcd88-a871-4245-a393-2843eafe6e02",
      "algorithm": "RSA",
      "purpose": 1
    }
  ]
}
```

## ۷ - ارسال صورتحساب

فرآیند ارسال صورتحساب هم مانند همهٔ فرآیندها در وبسرویس جمع‌آوری نیاز به احراز هویت فراخوانی کننده دارد. بنابراین از تکرار این مرحله صرف نظر می‌کنیم. فرض می‌کنیم عملیات گرفتن nonce امضای آن و ساخت توکن برای هر درخواست انجام می‌شود. فرض کنید یک صورتحساب الکترونیک در اختیار داریم. برای آشنایی با صورتحساب الکترونیکی و فیلدهای آن به سند [«دستورالعمل صدور صورتحساب](#)

شناسه سند RC_TICS.IS_v1.5	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
اردیبهشت ۱۴۰۴		

الکترونیکی» مراجعه نمایید. صورتحساب به فرم یک JSON دارای header (اطلاعات مربوط به خریدار و فروشنده و اطلاعات کلی صورتحساب)، body (لیست اقلام موجود در صورتحساب) و payments (اطلاعات مراحل پرداخت صورتحساب) می باشد.

در ابتدا باید با استفاده از شماره منحصر به فرد مالیاتی، صورتحساب را به شکل یکتا مشخص نماییم. سپس باید صورتحساب را امضا کنیم و بسته‌ی JWS تولید نماییم. در مرحله‌ی بعدی باید از صورتحساب امضا شده، به وسیله کلید عمومی سازمان (که از طریق GET server-information دریافت می‌گردد) بسته‌ی رمزشده JWE ساخته شود و سپس برای وب‌سرویس جمع‌آوری ارسال شود.

## ۱-۷ - جزئیات فرآیند ارسال صورتحساب

### ۱-۱-۱ - تولید شماره‌ی منحصر به فرد مالیاتی TaxId

برای آشنایی با چگونگی تولید شماره مالیاتی به سند قالب شناسه یکتای حافظه مالیاتی و شماره منحصر به فرد مالیاتی» مراجعه نمایید. همچنین در کیت توسعه نرم‌افزاری (SDK) به زبان‌های Java و .net توابعی جهت تولید شماره مالیاتی مطابق با الگوریتم‌های گفته شده پیاده‌سازی شده که نحوه‌ی استفاده از آن‌ها شرح داده خواهد شد.

### ۱-۲-۱ - امضای صورتحساب

امضای صورتحساب نیز مانند امضای توکن JWT می‌باشد بدین صورت که برای امضای صورتحساب باید یک بسته‌ی JWS ساخته شود که ساختار آن مانند جدول زیر باشد:

امضای صورتحساب – JWS	
<p>یک شیء JSON دارای فیلد‌های زیر:</p> <ul style="list-style-type: none"> <li>• alg: الگوریتم امضای RS256</li> <li>• x5c: لیستی که شامل گواهی امضای مودی باشد. کد شده به فرمت Base64</li> <li>• sigT: زمان امضای توکن</li> </ul> <p>Format: yyyy-MM-dd'T'HH:mm:ss'Z' Example: 2023-05-13T10:44:47Z</p>	<b>Header</b>

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	<p>سازمان امور ملی ایران</p>
---	--	------------------------------

<p>• crit: لیستی از فیلد های ضروری در قسمت Header. تنها شامل رشته‌ی "sigT" است.</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="color: #800080;">شیء JSON صورتحساب</th><th style="color: #FF0000;">Payload</th></tr> </thead> <tbody> <tr> <td style="padding: 10px;">           ورودی الگوریتم امضا:            ASCII (BASE64URL (UTF8 (JWS Protected Header))    '.'               BASE64URL (JWS Payload))            الگوریتم: RSASSA-PKCS1-v1_5 using SHA-256         </td><td style="padding: 10px; text-align: center;"> <b>Signature</b> </td></tr> </tbody> </table> <p>کلید خصوصی: کلید خصوصی متناظر با گواهی فرستاده شده در بخش Header</p>	شیء JSON صورتحساب	Payload	ورودی الگوریتم امضا: ASCII (BASE64URL (UTF8 (JWS Protected Header))    '.'    BASE64URL (JWS Payload)) الگوریتم: RSASSA-PKCS1-v1_5 using SHA-256	<b>Signature</b>	
شیء JSON صورتحساب	Payload				
ورودی الگوریتم امضا: ASCII (BASE64URL (UTF8 (JWS Protected Header))    '.'    BASE64URL (JWS Payload)) الگوریتم: RSASSA-PKCS1-v1_5 using SHA-256	<b>Signature</b>				

ساختار بسته JWS صورتحساب دقیقاً مانند توکن JWS می‌باشد. با این تفاوت که آن payload JWS می‌باشد. توجه کنید که رشته‌های Header و Payload باید به فرمت utf8 بوده و برای JSON صورتحساب می‌باشد. امضا و تولید بسته JWS به فرمت Base64URL کد شوند.

به عنوان نمونه فرض کنید Json صورتحساب ما بعد از تولید شماره مالیاتی به شکل زیر است:

```
{
  "header": {
    "taxid": "A1121604C220002F095011",
    "inno": "49321217",
    "indatim": 1683997837988,
    "inty": 1,
    "inp": 1,
    "ins": 1,
    "tins": "14003778990",
    "tob": 2,
    "bid": "10100302746",
    "tinb": "10100302746",
    "tprdis": 20000,
    "tdis": 500,
    "tadis": 19500,
    "tva": 1755,
    "todam": 0,
    "tbill": 21255,
    "setm": 2
  },
  "body": [
    {
      "sstid": "2710000138624",
      "ssts": "فولاد صنعت قطعات سرسیلندر سازی",
      "mu": 164,
      "am": 2,
      "fee": 10000,
      "prdis": 20000,
      "dis": 500,
      "adis": 19500,
      "vra": 9,
      "vam": 1755,
      "tsstam": 21255
    }
  ],
  "payments": []
}
```

حال یک شیء JWS می‌سازیم که آن مقدار زیر باشد:

```
{
  "crit": ["sigT"],
  "sigT": "2024-03-06T13:16:11Z",
  "x5c": [
    "MIIIE7DCCA9SgAwIBAgISAM4ybFjIYlezw/6Ly2CQYYNBMA0GCSqGSIB3DQEBCwUAMIG7MQswCQYDVQQGEwJJUjEZMBcGA1UECgwQTm9uLUDvdvmVybml1bnRhbDEkMCIGA1UECwwbQW1uYWZ6YXIGR29zdGFyLWUGU2hhcmImIENvMTQwMgYDVQQLDCTQYXJzU2lnbiJBjnRlcm11ZG1hdGUgQ2VydG1maWNhdGUgQXV0aG9yaXR5MTUwMwYDVQQDCxQYXJzU2lnbiBQcm12YXR1IEludGVybWVkaWF0ZSBTaWx2ZXIgQ0EgLSBHMzAeFw0yMzEwMTgwNjQyMTZaFw0yNDEwMTIwNjQyMTZaMIGyMSAwHgYDVQQDBdBbGkgU2hpcm1vaGFtYWRpIFtTaWduXTELMAkGA1UEBhMCSVIXDzANBgNVBCoMBti52YTbjDETMBEGA1UEBwwK2KrZh9ix2KfZhjEVMBMGA1UECgwMVW5hZmZpbG1hdGVkMRMwEQYDVQQFEwomMDIzNDU3NzA4MRMwEQYDVQQIDArYqtmtH2LHYp9mGMRowGAYDVQQEDBHYtNuM2LEg2YXYrdmF2K/bjDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIm7YPJLABiYHftOB9SsMps1OeFMJ5+brZLa4dE5cf404Qb2K6m+ITxT8sDO09mDLqbfxtCq1+ehlbAl/yugXdf5+rGYQYX/yaJf+vkaAq162vqdRvbVvkhNr1XI2rI+sXfGJBCGncskoVf7rm+RTciOmAA3ZhcjdU3jFmU1/Am8VBJ83kK8Qf8I6ZtFZhHL1Yp051xLv5QI4/lwmKxxEkmG+VgGV22Mkve3Yw1PoeMycoO110BvFd3iEnAUtHuIKF6cFwWia0hIJLvd+s/W7LuVQMNVYeu+J64zDqYBwDaSt4L+eofT6ksg6as1QSZdf/7VGyDGIqcjTet1E/C8CAwEAAAoB8DCB7TAdBgNVHQ4EFgQUepvjaOKnzm8N4C/+g1F4neodzaMwHwYDVR0jBBgwFoAUFMcoIHyJ0RZ/yrlp6IfJLEaC+lUwNAYDVR0fBC0wKzApoCegJYYjaHR0cDovL2wyLnBhcnNzaWduY2EuaXIVUFNFTDJDQS5jcmwwDgYDVR0PAQH/BAQDAgbAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMCMDcGCCsGAQUFBwEBBCswKTAnBggRbgeFBQcwAYYbaHR0cDovL2wyLnBhcnNzaWduY2EuaXI6ODEvMBQGA1UdIAQNMAswCQYHYIJsZQEBAjANBggkqhkiG9w0BAQsFAAOCAQEAcw2hdV1YN8xHXsQq4X6YwtgyUsK92CTILb/j2jYfIGXlwLCYxR6zPFuoqmjVG9Txs3NEPQirsVwqoIUzljTzNBU/W1PjeqPyWadQooRvg/64Ah88A8YJF3Yvv1Dax8rUANX+AQd0930xAr7hfCISTHFmhhw5GoJ153vh0idhekeK6//iwvLugPA9k0Qu0WObWsJ2Ctj2zWhCXMdz"
  ]
}
```

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	<p>سازمان امور ملی پارک هسته‌ای</p>
--	--	-------------------------------------

```
IajqkpEmyBJxe4yj9ZGyezjSmPb+khDgvEsbrOPcWy3WTSx80S3Shph18ywNQTRd6OximDXs14+1L0B1Zav6o0DpTlkF40OmoPkoZwQkJNxBrNrKWDek39vRR56yPP4p+04Ww=="] , "alg": "RS256"
"}]
```

و سپس آن را با استفاده از کلید خصوصی که در اختیار داریم امضا می‌کنیم. حال صورتحساب امضا

شده به صورت یک JWS در می‌آید:

```
eyJjcml0IjpbInNpz1QiXSwic2lnVCi6IjIwMjQtMDMtMDZUMTM6MTY6MTFaIiwiDVjIjpbIk1JSUU3RENDQT1TZ0f3SUJBZ01TQU00eWJGak1zbGV6dy82THkyQ1FZWU5CTUEwR0NTcUdTSWIzRFFFQkN3VUFNSUc3TVFzd0NRWURWUVFHRXdKS1VqRVpNQmNHQTFVRUNnd1FUbT11TFVkdmtVnlibTFSyM5SaGJERwtNQ01HQTFVRUN3d2JRVzF1WVdaN11YSwdSMj16ZEdGeUxXVWdVMmhoY21sbUlFTnZNVFF3TwdZRFZRUUxEQ3RRWVhKe1UybG5iaUJKYm5SbGNtMWxaR2xoZedVz1EyVn1kR2xtYdOaGRHVVwdRWFYwYUc5eWFYUjVNVFV3TxDzRFZRUUREQ3hRWVhKe1UybG5iaUJRY21sM11YUmxFJRwx1ZEdWeWJXVmthV0YwW1NCVGFxEdJaWE1nUTBFZ0xTQkhNekFlRncweU16RXdNVGd3TmpReU1UWmFGdzB5TkRFd01USxDoa1F5TVRaYU1JR31NU0F3SGdzRFZRUUREQmRCYkdrZ1UyaHBjbTF2YUdGdF1XUnBJRnRUYVdkdVhURUxNQwtHQTFVRUJoTUNTVk14RHpBTkJnTlZCQ29NQnPNTJZVGJjqREVUTUJFR0ExvUVCd3dLMktyWmg5axgyS2zaaGpFvk1CTudBMVVFQ2d3TVZXNWhabVpwYkdsaGRHVmtnuk13RVFZRFZRUUZFd293TURJek5EVTN0ekE0TVJnd0VRWURWUVFJREFyWXF0bUgyTEhZcD1tR01Sb3dHQV1EV1FRRURCSF10TnVNMkxFzzJZWF1yZG1GMksvYmpEQ0NB013RFFZSktrWklodmNOQVFFQkJRQRNrnZ0VQQRDQ0FRb0NnZ0VCQULtN11QSxkBYk15SGZ0T015U3NNchMxT2VGTUo1K2JSWkxhNGRFNWNmNDA0UWIySztK01UeFQ4c0RPMD1tRExxYmZ4VENxMstlaGxiQWwveXvnWGRGNStyr11RWVgveWFKZit2a2FBctE2MnzxZFJ2Y1z2a2hOcjFYSTJySStzWGZHskJjR25jZXNrb1ZmN3JtK1JUY21PbUFbm1poY2pkVTNqRm1VMS9BbThWQko4M2tLOFFmOEk2WnRGwmhITDFZcDA1MXhMVnM1UUk0L2x3bUt4a0VrbUcrVmdHVjIyTwt2ZTNzdFQb2VNeWMwTzExMEJ2RmQzaW1FbkFVdEh1SutGNmNGd1dpYTBoSUpMdmcry9XN0x1V1FNT1ZZZXUrSjY0ekRxWUJ3RGFTdDRMK2VvZlQ2a3NnNmFzbFFTWmRmLzdWR31ER01xY2pUZXQxRS9DOENBd0VBQWFPQjhEQ0I3VEFkQmdOVkhRNEVGZ1FVZXB2amFPS256bThONEMvK2cxRjRuZw9kemFnD0h3WURWUjBqQkJnd0ZvQVVGTwNPSUh5SjBSWi95cmxwNk1mskxFYUMrbFV3TkfZRFZSMGZCQzB3S3pBcg9DzWdKwv1qYUhSMGNEb3ZMMnd5TG5CaGnuTnphv2R1WTJFdWFYSXZVRk5mVERKRFFTNPjbx3RgdzRFzSMFBuuUgvQkFRREFnYkFNQ11HQTFVZEprRRIvd1FNTUFvR0NDc0dBUVVGQndNQ01EY0ddQ3NHQVFVRk3RUJCQ3N3S1RBbkJnZ3JCZ0VGQ1Fjd0FZWWJhSFIwY0Rvdkwyd31MbkJoy250emFXZHZVmKv1YvhJnk9ERXZNQ1FHQTFVZE1BUU5NQXN3Q1FZSF1JSnNaUVQCwpBTkJna3Foa21HOXcwQkFRc0ZBQU9DQVFFQWN3MmhkVjFZTjh4SFhzUXE0WDZZV3RneVVzSzkyQ1RJTGIvajJqWWZJR1hsd0xDWxhSNpQRnVvcW1qVkc5VHhzm05FUFPcnNwd3FvSVV6bGpUWm5CVS9XbFBqZXFQeVdhZFFvb1J2Zy82NEFoZDg4QThZSmYzWXZ2MURheDhyVUFOWCtBUWQwOTNPeEFyN2hmQ01TVEhGbWhodzVHb0oxNTN2aDBpZGhla2VLNi8vaAx2dTHvnuEE5azBRdtBXT2JXc0oyQ3RqMnpXaENyTWR6SWFqcWtwRW15Qkp4ZTR5ajlaR311empTbVBik2tORGd2RXNICK9QY1d5M1dUc3g4MFmzU2hwaGw4eXdoUVRsZDZPeGltRFhzMTQrbEwwQmxayXY2bzBEcFRsa0Y0ME9tb1Brb1p3UWtKTnhCck5yS1dEZUszOXZSuju2eVBQNHarMDRXdz09I10sImFsZyI6I1JtmjU2In0.eyjoZWfkZxiOnsidGF4awQioiJBMTeYMTYwNEMyMjAwMDJGMDk1MDExiawiaw5ubyI6IjQ5MzIxMjE3Iiwiaw5kYXRpbSI6MTY4Mzk5Nzgznzk4OCwiaW50eSI6MSwiaw5wiioxLCJpbmMiOjEsInRpbnMiOiiNDAwMzc3ODk5MCIsInRvYiI6MiwiYmlkiJoimTAxMDAzMDI3NDYiLCJ0aW5iIjoiMTAxMDAzmDI3NDYiLCJ0cHJkaXMiOjIwMDAwLCJ0ZGlzIjoi1MDAsInRhZGlzIjoxOTUwMCwidHzhbSI6MTc1NSwidG9kYW0iOjAsInRiaWxsIjjoyMTI1NSwic2V0bSI6Mn0sImJvZhkiOlt7InNzdG1kIjoiMjcxMDAwMDEzODYyNCIsInNzdHQiOiLy9ix2LPbjNmE2YbYr9ixINmC2LfYudin2Kog2LXZhti52Kog2YHzinM2KfYryDYs9in2LLbjCisIm11IjoiMTY0IiwiYw0iOjIsImZlZSI6MTAwMDAsInByZG1zIjjoyMDAwMCwiZG1zIjoi1MDAsImFkaXMiOjE5NTAwLCJ2cmEiOjksInZhbsI6MTc1NSwidHNzdGftIjjoyMTI1NX1dLCJwYXltZW50cyI6W119.AVPw0w2IG7BJ5zglQYrP_vvBT1wX0eB4ZP77vvQkTN2At-zb8hpFegG-uqui99cvR4i27GVnKcMpLBNVmMrL4FODTXqKn053bJ8oPJhbnUFhIkOAcOrPUotm05jsWvocAL07Bh-m8B7nQG7d-RLEXViwbaCmMI7hzMCBzMm3P0Sr2cBVDrK8FUR_8VHb219gUm52A4Wy8i4moHc1Gi_6503vrNX9bN3DiJSS_me5WOise0GjglB3zHTMzE6MAZMpBbVJYfJOK-h-RKJaWLAlIVzYbYmhVMBfuxFB5Q9D1qDsvc0ie4Nn3Qs0sMVPcNO335ANSMu7wgFPqYmEK5aEw
```

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امنیت ملی ایران</p>
---	---	-------------------------------

توجه کنید که بررسی اعتبار امضا و گواهی امضا کننده صورتحساب نیز عیناً همانند بررسی توکن JWS می‌باشد و در کنار بررسی گواهی امضا صادرکننده صورتحساب و تاریخ انقضای گواهی، از سرور OCSP و CRL صادرکننده گواهی استعلامات لازم برای اطمینان نسبت به اعتبار و صحت گواهی گرفته می‌شود.

لازم به ذکر است گواهی استفاده شده در فرآیند امضای صورتحساب می‌بایست معترض بوده و کد ملی/شناسه ملی موجود در گواهی<sup>۷</sup> دسترسی ارسال صورتحساب برای شناسه یکتاوی حافظه مالیاتی مربوطه را داشته باشد.

### ۷-۱-۳ - رمزگذاری صورتحساب

در مرحله‌ی بعد باید صورتحساب امضا شده را رمزگذاری کنیم. این کار باعث می‌شود هیچ شخص دیگری به جز سرور سامانه‌ی مودیان توانایی بازکردن و مشاهده محتويات صورتحساب را نداشته باشد. الگوریتم AES/GCM/NoPadding AES256-GCM رمزگذاری مورد استفاده در این مرحله (AES/GCM/NoPadding) می‌باشد و کلید RSAES OAEP using SHA-256 and MGF1 with (RSA-OAEP-256) نیز از طریق الگوریتم SHA-256 رمز می‌شود که این فرآیند بر اساس استاندارد JWE انجام می‌شود. الگوریتم رمزگذاری AES256-GCM دارای ۴ ورودی و ۲ خروجی است. ورودی‌های الگوریتم عبارتند از محتوای بسته یا همان payload، کلید متقارن، iv و داده اضافی احراز هویت AAD (Additional Authentication Data). خروجی‌های الگوریتم عبارتند از بسته‌ی رمزشده و تگ احراز هویت (Authentication tag). ابتدا یک کلید ۲۵۶ بیتی AES به همراه ۹۶ بیت iv (یا همان Initial Vector) تولید می‌شود. داده اولیه AAD هم از روی header ساخته می‌شود و در کنار محتوای بسته یا همان Payload (رشته‌ی JWS صورتحساب امضا شده) به عنوان ورودی به الگوریتم داده می‌شود تا داده رمز شده و Authentication Tag محاسبه شود. سپس خود کلید با الگوریتم RSA و به وسیله کلید عمومی سازمان رمز می‌شود. در نهایت صورتحساب رمزشده در کنار کلید AES رمز شده، شناسه کلید عمومی سازمان، iv و تگ شناسایی، یک بسته JWE را تشکیل می‌دهند که می‌توان آن را برای وب‌سرویس سامانه‌ی مودیان ارسال نمود.

<sup>۷</sup> فیلد SUBJECT در قسمت SERIALNUMBER گواهی امضاء

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	<p>سازمان امور ملیا و کشور</p>
---	--	--------------------------------

## JWE ساختار شیء

بسته‌ی رمز شده – JWE	
<p>یک شیء Json دارای فیلدهای زیر:</p> <ul style="list-style-type: none"> <li>• "alg": مقدار RSA-OAEP-256</li> <li>• "enc": مقدار A256GCM</li> <li>• "kid": شناسه کلید عمومی رمزگذاری سامانه مودیان</li> </ul> <p>نمونه:</p> <pre>{"alg": "RSA-OAEP-256", "enc": "A256GCM", "kid": "6a2bcd88-a871-4245-a393-2843eafe6e02"}</pre> <p>کلید متقارن رمزگذاری AES به طول ۳۲ بایت (۲۵۶ بیت) را با استفاده از الگوریتم RSAES OAEP using SHA-256 and MGF1 with RSA-OAEP-256 (SHA-256) با کلید عمومی رمزگذاری سامانه مودیان به طول ۴۰۹۶ بیت، رمز کنیم. کلید رمز شده ۵۱۲ بایت طول دارد که Base64URL Encoded آن را در این قسمت قرار می‌دهیم.</p> <p>Encode شده‌ی ۱۲ بایت (۹۶ بیت) iv به فرمت Base64URL که رشته‌ای به طول ۱۶ کاراکتر می‌شود.</p> <p>رشته‌ی JWS صورتحساب امضا شده که با استفاده از کلید متقارن و با الگوریتم AES256-GCM رمز می‌شود.</p> <p>تگی که به منظور اطمینان از دستکاری نشدن محتوای پیام رمز شده و کلیدها استفاده می‌شود.</p>	<b>Header</b> <b>سرآیند</b>
<p>کلید متقارن رمز شده</p>	<b>Encrypted Symmetric Key</b>
<p>Initial Vector</p>	<b>Payload</b> <b>محتوای رمز شده</b>
<p>Authentication Tag</p>	<b>Tگ شناسایی</b>

برای شناخت بیشتر نسبت به ساختار JWE سند RFC7516 را مشاهده کنند:

<https://www.rfc-editor.org/rfc/rfc7516>

مطابق این استاندارد قالب چیدمان بسته JWE به صورت زیر است:

```
BASE64URL(UTF8(JWE Protected Header))||'.'||  
BASE64URL(JWE Encrypted Key)||'.'||  
BASE64URL(JWE Initialization Vector)||'.'||  
BASE64URL(JWE Ciphertext)||'.'||  
BASE64URL(JWE Authentication Tag)
```

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	 <p>سازمان امور ملیان کشور</p>
--	--	---

مراحل رمزگذاری صورتحساب:

سرآیند JWE به فرمت utf-8 برابر است با:

```
{"alg": "RSA-OAEP-256", "enc": "A256GCM", "kid": "6a2bcd88-a871-4245-a393-2843eafe6e02"}
```

که Encode شده آن به فرمت Base64URL می‌شود:

```
eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBmJU2R0NNIiwia2lkIjoiNmEyYmNkODgtYTg3MS00MjQ1LWEzOTMtMjg0M2VhZmU2ZTAyIn0
```

توجه کنید که رشته‌ی سرآیند (header) حتماً باید به فرمت utf-8 باشد.

حال یک کلید متقارن تولید می‌کنیم که Encode شده آن به فرمت Base64URL برابر است با:

```
_hm__fdwWlcK2FiFuuOHcRHqvKeYrd9_tzAdUI9IK5E
```

سپس این کلید را با کلید عمومی رمزگذاری سامانه مودیان به طول ۴۰۹۶ بیت، رمز می‌کنیم. این کلید از API دریافت اطلاعات سرور دریافت می‌شود و مقدار آن به فرمت Base64 برابر است با:

```
MIICIJANBgkqhkiG9w0BAQEFAOCAg8AMICCgKCAGEAxdzREOEfk3vBQogDPGTMqdDQ7t0oDhuKMZkA+WmlhzjjhAGfSUOUdVOKRoUEQwP8oUcXRmYzcvCUGcf0RT5iz7HbovqH+bIeJwT4rmLmFcbfPke+E3DLUxOtIZifEXrKXWgSVPkRnhMgym6UiAtnzwA1rmKstJoWpk9Nv34CYgTk8DKQN5jQJqb9L/Ng0zOEEtI3za424tsd9zv/kP4/SaSnbbnj0evqsZ29X6aBypvnTnwH9t3gbWM4I9eAVQhPYClawHTqvadz/O/feqfm06QBFnCgL+CBdjLs30xQSLsPICjn1V1jMzoTznAabWP6FRzzj6C2sxw9a/WwlXrKn3gldZ7Ctv6Jso72cEeCeUI1tzHMDJPU3Qy12RQzaXujpMhCz1DVa47RvqiumpTNyK9HfFIDhgoupfkxT14XLD165S55MF6HuQvo/RHSbBJ93FQ+2/x/Q2MNGB3BXOjNwM2pj3ojbDv3pj9CHzvaYQUYM1yOcFmIJqJ72uvFv9Jx9iTObaNNF6pl52ADmh85GTAH1hz+4pR/E9IAxUI1/YiUneYu0G4tiDY4ZXykJYNknNfhSgxmn/gPHT+7kL31nyxgjiEEhK0B0vagWvdRCNJSNGWpLtlq4F1CWTAnPI5ctiFgq925e+sySjNaORCoHraBXNEWyiHT2hu5ZipIW2cCAwEAAQ==
```

و حاصل رمز شده کلید متقارن با کلید عمومی به فرمت Base64URL سازمان می‌شود. قابل توجه است که خروجی رمز شده الگوریتم RSA-OAEP-256 با ورودهای یکسان، متقاوت خواهد بود:

```
1Rs_vcZlauJs4VwED3wZGr3wJDbg8It9zBStuJgqf7TiGs3kUCSulPwA6jRA-8xuHTpNtKr1w0hsNbUhxs-3BL5zGaDzsSekA1AZVevVy2qOrfId60xLoB81SpVnSRR_K3jRHDwfH_ZDgZqMoM2mv6qFvb8GgGFV59_jIkhtcX73Y6iqe3NCask2CT0Ine3SUFVxt_OBqnBCwgDLrauGyisQbpVN1JJRjsWPeyXA00Wv1ECnRSLS93-prnMrfLTU_JHUyU304-cq7gVu7OATP1NB78L8m0-MiIF_tr0mpbaEneOLDbmNYt2UVgn1thJsvh5Na30GKY5t-ISHoWhX-DvvHp3KTEpp0bkC8IczTt-jg-2vdYhyM7Sz1H0c9w2EvSSryVsAVonOoj14yWeaNhP_7mk09hgu1MUkr91Tfr-U1k3zFHyC1fJzHj3t3uebS2mFDEyuao7K4omC335_vYsCi6kRSU421AW1_8V21Rxas2VDBQbgoCqr3UQQxsosRIG3v1-OBgTgZ9s1EGZnEihaptab-7IeqnXIbhZNA8Onzy0wKW2S6r8M2eDd01QhGaDPGXcdWtOpC-Q-
```

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	<p>سازمان امور ملیان اکثر</p>
---	--	-------------------------------

cvu9MJTp4MRDx5dYe2rRQaI\_A7WS5vJGkjwdRRpfhaJhGoXA7Wc6eUmB\_UFOvPfsGQdFXPBUB3vh6jPfsER6hnXjU

مقدار IV تولید شده برای رمزگذاری محتوای اصلی با کلید AES به فرمت Base64URL برابر است با:

75ZoCO0VRqIWRYAs

همچنین برای ایجاد تگ شناسایی نیاز به داده اضافی احراز هویت یا همان Additional ) AAD ( داریم که مقدار آن از طریق محاسبه مقدار ASCII سرآیند (Authenticated DataEncode (Header) شده به فرمت Base64URL به دست می آید:

Header: {"alg": "RSA-OAEP-256", "enc": "A256GCM", "kid": "6a2bcd88-a871-4245-a393-2843eafe6e02"}

Base64URL(Header): eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBmjU2R0NNIiwia21kijoInMxEyYmNkODgtYTg3MS00MjQ1LWEzOTMtMjg0M2VhZmU2ZTAyIn0

AAD = ASCII(Base64URL(Header)): [101, 121, 74, 104, 98, 71, 99, 105, 79, 105, 74, 83, 85, 48, 69, 116, 84, 48, 70, 70, 85, 67, 48, 121, 78, 84, 89, 105, 76, 67, 74, 108, 98, 109, 77, 105, 79, 105, 74, 66, 77, 106, 85, 50, 82, 48, 78, 78, 73, 105, 119, 105, 97, 50, 108, 107, 73, 106, 111, 105, 78, 109, 69, 121, 89, 109, 78, 107, 79, 68, 103, 116, 89, 84, 103, 51, 77, 83, 48, 48, 77, 106, 81, 49, 76, 87, 69, 122, 79, 84, 77, 116, 77, 106, 103, 48, 77, 50, 86, 104, 90, 109, 85, 50, 90, 84, 64, 121, 73, 110, 48]

محتوای بسته که همان صورتحساب امضا شده است را با کلید متقارن تولید شده و الگوریتم AES256-GCM

رمز می کنیم و حاصل به فرمت Base64URL برابر است با:

GiB15WaorEeK77gX1Tr-  
141X0520tRcvrhp8D9cHcfYLTIonEo3MXYQ46Z8QTPv2ueCdiKztQDngTuczGGY3lvelcz-  
tHqeAJZ92UG9cjouMVE7IY29ML7OrzPy66GJsVb3BZnmIm6vDNEMF9AL8LH3y-  
H4rk9JmZjQbrRIU2AbmTGwRK0\_FnQD660b-4nEMKfc51h9bk-  
dc8as3\_OxFH2b0KxaiZDki8pDLumCFPQ9U9pfU7KUmkFl09FGF3FpryGX5DzEE\_YprotK6lcEr9  
f8U5ooHS\_PF06pprnL\_CkXtimdJENJgghk-  
5xdZfdIMlR4ghYPDTr\_frfE0GjmroEaWOaoM3qXwDhdUFs1nb\_48KAUOQY1ebgd9Ngi\_ed-  
rh517TAj1wPCmqnPEY9SYIpeorurSw1MPPpI9NN-bjjBUhW1a4RxkCt5UeHDS--  
bvrkPqD5Dai0Qg2RD7n8cm6pzHKcKO16WpXSSFhIjK1-  
1\_kevoprXPIEHtWk3PBSXYWDz15Gc\_ET-aw2CF6xgWkUi-  
vw512\_ySvs66grxGqubBQkOOxLLyUEmcxedPSCSs6g4eNqf-  
SES0yZ9NR4uBs3WBsq2h0Ftrn5ZKnimDQKtoU0LJvscjXBso6ckAVuvjBily4zKgr07FjJ9zn-  
9xkStotxms0czBo-  
fOsVunTuKypLBvTiwV4uykqUnsxbyOtuUvr10kLK1dma4F9q1giXRqfoMynlo7seRDTrrTkBh\_D  
krF-  
AzNhZG3o1TC5bHUtWn5crc2dw3FkS4UMelunQkusFL44MRqY3qbn\_iP4NY8X3bWTWtp31kiFxKt  
ATTiZG\_lvi5om1QwcA7a\_mYQw47EjjvGTiSJQsfDM8d2WB1VDOV65xgcqy70QVRPxftO6jJu-  
X1MGd-RN2Lb\_crLsnJGJ6kpdhqyF7ts\_3gbWvryzKLJyDe2HM3izN6Kw0U4Ba-\_\_YOMPV-  
mJECsVC5KUw9jRYhw6tdYSU41LXKRdnMyh-

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	 <p>سازمان امور ملیان اکثر</p>
---	--	---

cjRyuv4V347DOR280aGWsbqpqaDp4mdtkaABARhtO5BhbzeSnHnEjTVZmdn8H5WifzGvqHCiGA  
z752CNNO00OwCbpVoWJcq78XndubsxsXzkcg0XvsDxnKzdBdRkoYyTEd5tMODxUZw\_tpbXNQZF  
FwAB4ph\_FtoYC0j50kGhEola6h7jguoFJu0CewloGSkvvqu2Ht4G9IfDkFs0tMTvdjHJJGWPdj9  
nQ\_Mzn0QkKBPhGLM50yUtosIVd1FvrHCJuhkt3qsAP6OTHvgDswELnLMcOsorB2qdVp6YSAOT3Z  
uRc6Bawwd5S78wd\_o4ISW9pNMxNbHPueiXI\_N48S9Zcb2ktwH6dB3rbkRwgXCEwcPheX8s5ik32  
5PbY5RAAs29fj45yISSZ-  
6x1g9BwBXjg81TkNg18\_6j0aI8ZZmDjL1EyjK0obj9UpQUfjreakNAGhxSa5S\_ethyl63Bs6\_En  
XyzOKDP5sPmlyBgJ6RjXRSmVI8zqA1ETazPY93PYql\_PqADQm48\_Ocs1h\_djjNNBHeA8ucYelX1  
T8tcD-ENwrvJw8\_2u1A1DWX-  
FucPGQQLZc4PkW04OCUEb1xDUsJFzedhX0cKEQr\_b9zxhVT3C09yr3q6FyhqrYF892Kq106PmXB  
VEZrb-Q0piVZyozeordNJGRE016r8A10hnc-KgUlkdZrxee\_zzk9aV08CU01-  
fvBRCGOR12v\_EAcY17pnyfnCKmZH3u3Iq5D7-  
T3JHJSZz2NuUFrCok81L87X0YbRCscW164VAEsF1QolakktKt8cNRQwj\_95rtt1Ka06Fdg6Q-  
VK9NskncRKKn1WcIQT6Ec6eTmr1Ng7JaQ7dqkEh\_zThM8ife-  
Ak6jVdpMiHZ4Nvd1OndCPbi1r7zFNrUeRI0BK5PWF0JA90YAnMJ3B7DkrAMyLhZMkKXp4UjEZSQ  
hBhe\_lnD9VxL3rZcmRqEctFVmsTnyRZY-  
pZ1Sx8gS\_99WXrtNqD11R3njeHWJsCi35GoJJwWh3BFCJvsyeQcmsIkkN4RdBwj\_B-  
ZpUKJn1gvho2E7PPkvuMpMPSWr1czptCpzamAY2pTjBgmQ5NWDnxN87fUZN9YaJYMcqD7kb-  
kooJuNWw7TcF-YPo\_31UHHWd3mKzBFVUeYEqqJBA-  
9KroMQzfC7hc5QqkaA\_oGVn0\_8\_Aexx7fNDdXc6yRzM\_msfGsb06pMYegbEijS5F3DaopvpAmwd  
Bbf1DRUIGSKpfODn9DNGB2BoqNn1mNPCu\_BsqGuPvF3RzgxP-1MoCI3XF7RxG1DYr-  
bTPsV6pyzinV5HaGSNRorYkXchaXh119k4d9pfu\_4uXeASFVG6WxzdpVwb\_w769VQdVYL7KG0u4  
uC\_MhWDH0w1DVEFySffBNPpZ6Z\_1LYkbc8epocBH9HjJVFByp4ggVieVuDlx\_tkK6QUwSPZT136  
Be4uVf9luAJXZfn3IkMbJ8KuRfLjwBE3N4MnjXbz4RHN5dZwaSJftRgYo\_DaJPiqcGz1H3dB5B4  
i0A7bLA4H1TEIKLPom-  
A1GnpRruGdoF7dD3dhx8HOKUT7ny7zMrYQWI86bmRzubnMZmi87GguvCoCP7o7ATMJIGprSDmg-  
3TJ5FGyeXaNZRZ01EP1Dhc6uh19Pm\_PYP718tKg5Z\_dGgnFWwJp2SDweU7kvWgEUePJVa-  
HKd7iiRGP-  
2cttS8ak4z1q\_OjKkFRHi6A2uZ95Yg0dkWgBbHgCHbbuM5oBmIztFixmnHeoTrV3HPbBPw2jEX\_-  
XINhFVcYnfclefs0Gh-  
jKA4wrCgStq5bXRhMC5degaoQ0Sb5eY\_S\_Ehpz1yoA\_JYDHp6t8FFnSMTNbM9LfoBTgZDdlrRmw  
d2dBVJxzbkhTpXo4dpShFRsL1vs0GV3wdELBuzMb3UaTyu-  
rJy\_DObIPE8pmlC1NS\_WhRVXB0gJf91MaaIup\_Fx7tJzSbqiNG9mFj6SQvMk0HvAyI195NpyF  
NX33x5NLFnF6125mZdn6MY6nLPeNu9P1yEadZ8uXnMtfrAOuN83yS2XZDWKHPYSJOaVcsGAjRr  
cGLpulp-dcx1g0XVQgNR0KzaH7J3zbRJ-Lqf7V6w9aYT1JnHk21bof2oGp9NaWN1-  
Tq1OEvrAk3-  
EqzyCigOG5A2YZdoRR\_1rlCxfNCXz0dtRwM07IX\_kEEEKHTs4lk970YTSa\_SdhYNMUN0QPBLkjT  
ts\_YMnx8Y2wFumFy9Ji3K5o2GHB5nc0a1Di0Si9gNEpFjv6pT\_Tk9NDIFUBAwv8oV\_qp41qFqSp  
A9g6G51madn0K6sonvAsR1DWNjxSBr0pg1stgWWCRe3Ucp\_b9PhZht1rSuJsZynEqLCf9ZLn2lx  
fugLbI0dvaNZxki2NtNHCv\_CsiMFo76rC5SwCJ5uTtD64z53s2txbOPmhWpIGE63OKi3fQSZz5H  
ZdBbidIRcM3vCEseMNw1A27F7\_BCIN6o9tzd-1X0Zkvh08Wts2d-c1Fs-  
x5ssLWeoMPpGvnFjZ9pQBD8EyK34JsA5qPTVjLOD62ZRph8PdkijIoE0es4QMyleVbUe9rbscIN  
F2m5YSHiRWWM5MFSpDFmT67EtriseeWQnVNQUT31\_chDRut92yv2G3seSa8HHLW0Gmq7W7hUUG  
uxLbUSVv74U7\_55vpQM0fuRhJ7khTbZioN-  
wBp32Zyy\_phgMi5s0qV351PoCzpZ7ueQwbsS6kvABCj2PjoeQL2trqrjcfkPfLPUksETgkVrgvi  
jt55bzKmUG624fv1zJbgSt7t3rrPiVQyKflW0YJcx-  
39sKD1CQeEFpQp\_7gnf7LoKKVPAISDLSSCHJro6R5Vm74INsQQjGn-  
fH55R2sS4GVw74DfwF1k7wp9Upw3Jj1gQ9MhRpVjUd98CprL-  
jjdn4k4CuHxZPXEoXEfkvC8PO4HmDN1Od-  
3ShVrilhJ1gLFpuM1814Oy1Uju9bhHEM8R28YL7ftgWvtzhMkdw3BPM05Uzo29xAss\_GZeDikFl

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	<p>سازمان امور مالیاتی کشور</p>
--	--	---------------------------------

db2E7CoZu3evhnrMsk9KWGbbrxcAZDFR1zhNJHJBVFVppjpxgoXy6Br3LAtZBnu217zt5mfAF08h  
 EG0baz-MS0hPahtcoE3S7c5xPcV4wTmmX\_r9pE\_eg-  
 6tyiylj5I9h0pgUMt0gAgRSNA8VP5YLvoDv5D3eMhK\_ZzTQtQGEQulpA86uPKjImusrAe4XAAbFE  
 fWIPZ--S6xkYacgCzGjqfAQOIInmRLg\_fOcmuy2atMbCX9RF66rbGhOTwIY-HEBUAeIA9cY\_AL-  
 rb78ErzcKhRodnAN3XXq-rpA9709UjBiFm\_SEPGEsA6HlmxDOPFubEt1g-  
 36CxG41OLaKSEAXPUm105xNWUHS\_xOaT55mq4DgaX\_3cn8q6za9729x3PiGwtw0Lh1hH-  
 sezEb7wkSW0hJJoXkrKAMKD\_HcaV7cAcwiMEvvE3sX\_JQ

همچنین خروجی Authentication Tag عملیات رمزگذاری بسته با iv و aad داده شده به فرمت Base64URL برابر است با:

m0uVEEEqSLHJRbG-xLoSyA

از کنار هم گذاشتن این مقادیر به ترتیب header، کلید متقارن رمز شده با کلید سازمان، iv، بسته‌ی رمز شده با کلید متقارن تولید شده و تگ شناسایی بسته‌ی JWE ساخته می‌شود:

eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBmjU2R0NNIiwick21kIjoiNmEyYmNkO  
 DgtYTg3MS00MjQ1LWEzOTMtMjg0M2VhZmU2ZTAyIn0.1Rs\_vcZlauJs4VwED3wZGr3wJDbg8It9  
 zBStuJgqf7TiGs3kUCSu1PwA6jRA-8xuHTpNtKrlw0hsNbUhxs-  
 3BL5zGaDzsSekA1AZVevVy2qOrfId6OxL0b81SpVnSRR\_K3jRHDWFH\_ZDgZqMoM2mv6qFvb8GgG  
 FV59\_jIkhtx73Y6iqe3NCask2CT01ne3SUFWxt\_OBqnBCwgDLrauGyisQbpVN1JJRjsWPeyXA0  
 0Wv1ECnRSLS93-prnMrfLTU\_JHUYU304-cq7gVu70ATP1NB78L8m0-  
 MiIF\_tr0mpbaEneOLDbmNYt2UVgn1thJsvh5Na30GKY5t-ISHoWhX-  
 DvVhp3KTEpp0bkC8IczT-jg-  
 2vdYhyM7Sz1H0c9w2EvSSryYsAVonOoj14yWeaNhP\_7mk09hgu1MUkr91Tfr-  
 U1k3zFHycC1fJzHj3t3uebS2mFDEyua07K4omC335\_VYsCi6kRSU421AW1\_8V21RxaS2VDBQbgo  
 Cqr3UQQxsosRIG3v1-OBgTgZ9s1EGZnEihaptab-  
 7IeqnXIbhZNA8Onzy0wKW2S6r8M2eDd01QhGaDPGXcdWtOpC-Q-  
 cvu9MJTp4MRDx5dYe2rRQaI\_A7WS5vJGkjwdRRpfhaJhGoXA7Wc6eUmB\_UFOvPfsGQdFXPBUB3v  
 h6jPfsER6hnXju.75zoCO0VRqIWRyAs.GiB15WaorEeK77gX1Tr-  
 141X0520tRcvrhp8D9chCFYLTionEc3MXYQ46Z8QTPv2ueCdiKztQDngTuczGGY3lve1cz-  
 tHqeAJZ92UG9cjouMVE7IY29ML70rzPy66GJsVb3BZnmIm6vDNEMF9AL8LH3y-  
 H4rk9JmZjQbrRIU2AbmTGwRK0\_FnQD660b-4nEMKfc51h9bk-  
 dc8as3\_OxFH2b0KxaiZDki8pDLumCFPQ9U9pfU7KUmkf1o9FGF3FpryGX5DzEE\_YprotK6lcEr9  
 f8U5ooHS\_PF06pprnL\_CkXtimdJEJgghk-  
 5xdZfdIMlR4ghYPDT\_rfE0GjmroEaWOaoM3qXwDhdUFs1nb\_48KAUOQY1ebgd9Ngi\_ed-  
 rh517TAj1wPCmqnPEY9SYIPEorurSw1MPPpI9NN-bjjBUhW1a4RxkCt5UeHDS--  
 bvrkPqD5DaiOQg2RD7n8cm6pzHKcKO16WpXSSfhIjk1-  
 l\_kevoprXPIEhtWik3PBSXYWDz15Gc\_ET-aw2CF6xgWkUi-  
 vw512\_ySvs66grxGqubBQkOOxLLyUEmcxedPSCSs6g4eNqf-  
 SES0yZ9NR4uBs3WBsq2h0Ftrn5ZKniMDQKtoU0LJvscjXBso6ckAVuvjBily4zKgr07FjJ9zn-  
 9xkStotxms0czBo-  
 fOsVunTuKypLBvTiwV4uykqUnsxbyOtuUvr10kLK1dma4F9qlgiXRqfoMynlo7seRDTrrTkBh\_D  
 krF-  
 AzNhZG3o1TC5bHUtWn5crc2dw3FkS4UMelunQkusFL44MRqY3qbn\_iP4NY8X3bWTWtp31kiFxKt  
 ATTiZG\_lvi5om1QwcA7a\_mYQw47EjjvGTiSJQsfDM8d2WB1VDOV65xgcqy7OQVRPxfTo6jJu-  
 X1MGd-RN2Lb\_crLsnJGJ6kpdhqyF7ts\_3gbWvryzKLJyDe2HM3izN6Kw0U4Ba-\_\_YOMPV-  
 mJECsVC5KUw9jRYhw6tdYSU41LXKRdnMyh-  
 cjRyuv4V347DOR280aGWsbqpqaDp4mdtkaABARht05BhbzeSnHnEjTVZmdn8H5WifzGvqHCiGA  
 z752CNNO000owCbpVoW2Jcq78XndubsxsXzkcq0XvsDxnKzdBdRkoYyTED5tMODxUZw\_tpbXNQZF

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	<p>سازمان امور ملیان اکثر</p>
---	--	-------------------------------

FwAB4ph\_FtoYC0j5OkGhEola6h7jguoFJu0CewloGSkvvqu2Ht4G9IfDkFs0tMTvdjHJJGWPdj9nQ\_Mzn0QkKBPhGLM50yUtosIVd1FvrHCJuhkt3qsAP6OTHvgDswELnLMcOsorB2qdVp6YSAOT3ZuRc6Bawwd5S78wd\_o4ISW9pNMxNbHPueiXI\_N48S9Zcb2ktwH6dB3rbkRwgXCEWcPheX8s5ik325PbY5RAs29fj45yISSZ-  
6x1g9BwBXjg81TkNg18\_6j0aI8ZZmDjL1EyjK0obj9UpQUfjreakNAGhxSa5S\_ethyl63Bs6\_EnXyzOKDP5sPmlyBgJ6RjXRSmVI8zqA1ETazPY93PYql\_PqADQm48\_Ocs1h\_djjNNBHeA8ucYelX1T8tcD-ENwrvJw8\_2u1A1DWX-  
FucPGQQLzC4PkW04OCUeBlxDUsJFzedhX0cKEQr\_b9zxhVT3C09yr3q6FyhqrYF892Kq106PmXBVEZrb-Q0piVZyozeordNJGRE016r8A10hnc-KgUlkdZrxee\_zzk9aV08CU01-fvBRCGOR12v\_EAcY17pnyfnCKmZH3u3Iq5D7-T3JHJSzz2NuUFrCok81L87X0YbRCscW164VAEsF1QolakktKt8cNRQwj\_95rtt1Ka06Fdg6Q-VK9NsKncRKKn1WcIQT6Ec6eTmr1Ng7JaQ7dqkEh\_zThM8ifE-Ak6jVdpMiHZ4Nvd1OndCPbi1r7zFNrUeRI0BK5PWF0JA90YAnMJ3B7DkrAMyLhZMKXp4UjEZSQhBhe\_lnD9VxL3rZcmRqEctFVmstNtyRZY-pZ1Sx8gs\_99WXrtNqD11R3njeHWJsCi35GoJJwWh3BFCJvsyeQcmsIkkN4RdBrwj\_B-ZpuUKJn1gvho2E7PPkvuMpMPSWr1c1zptCpzamAY2pTjBgmQ5NWDnxN87fUZN9YaJYMcqD7kb-kooJuNWw7TcF-YPo\_31UHHWd3mKzBFUeYEqqJBA-  
9KroMQzfC7hc5QQkaA\_oGVn0\_8\_AexX7fNddXc6yRzM\_msfsGsbO6pMYegbEijS5F3DaopvpAmwdBbF1DRUIGSKpfODn9DNGB2BoqNn1mNPCu\_BsqGuPvF3RzgxP-1MoCI3XF7RxG1DYr-  
bTPsV6pyzinV5HaGSNRorYkXchaXh119k4d9pfu\_4uXeASFVG6WxzdpVwb\_w769VQdVYL7KG0u4uC\_MhWDH0w1DVEFySffBNPpZ6Z\_1LYkbc8epocBH9HjJVFByp4ggVieVuDlX\_tkK6QUwSPZT136Be4uVf9luAJXZfn3IkMb8KuRfLjwBE3N4MnjXbz4RHN5dZwaSJftRgYo\_DaJPiqcGz1H3dB5B4i0A7bLA4H1TEIKLPom-  
A1GnpRruGdoF7dD3dhx8HOKUT7ny7zMrYQWI86bmRzubnMZmi87GguvCoCP7o7ATMJIGprSDmg-3TJ5FGyeXaNZR0LEP1Dhc6uh19Pm\_PYP718tKg5Z\_dGgnFWwJp2SDweU7kvWgEUePJVa-HKd7iIRGP-  
2cttS8ak4z1q\_OjKkFRHi6A2uZ95Yg0dkWgBbHgCHbbuM5oBmIztFixmnHeoTrV3HPbBPw2jEX\_XINhFVcYnfclefs0Gh-jKA4wrCgStq5bXRhMC5degaoQ0Sb5eY\_S\_Ehpz1yoA\_JYDHp6t8FfnSMTNbM9LfoBTgZDdlrRmw d2dBVJxzbhTpXo4dpShFRsL1vs0GV3wdELBuzMb3UaTyu-rJy\_DOb1fPE8pm1C1NS2\_WhrVXB0gJf91MaaIup\_Fx7tJzSbqiNG9mFj6SQvMk0HvAyI195NpyF NX33x5NLFnF6125mZdn6MY6nLPeNu9P1yEadZ8uXnMtwfrAOuN83yS2XZDWKHPYSJOaVcsGAjRrcGLpulp-dcx1g0XVQgNR0KzaH7J3zbRJ-Lqf7V6w9aYT1JnHk21bof2oGp9NaWN1-Tq1OEvrAk3-EqzyCigOG5A2YZdoRR\_1rlCxfNCXz0dtRwM07IX\_kEEEKHTs41k970YTSa\_SdhYNMUN0QPBLkjT ts\_YMnx8Y2wFumFy9Ji3K5o2GHB5nc0alDioSi9gNEpFjv6pT\_Tk9NDIFUBAwv8oV\_qp41qFqSp A9g6G51madn0K6sonvAsR1DWNjxSBropg1stgWWCR3Ucp\_b9PhZht1rSuJsZynEqLCf9ZLn21xfugLbIOdvaNZxki2NtNHcv\_CsiMf076rC5SwCJ5uTtD64z53s2txbOPmhWpIGE63OKi3fQSzz5HZdBbidIRcM3vCEseMNw1A27F7\_BCIN6o9tZd-1X0Zkvh08Wts2d-c1Fs-x5ssLWeoMPpGvnFjZ9pQBD8EyK34JsA5qPTVjLOD62ZRph8PdkijIoE0es4QMyleVbUe9rbscIN F2m5YSHiRWWM5MFSpDFmT67EtriseeWQnVNQ TU31\_chDRut92yv2G3seSa8HMLW0Gmq7W7hUUG uxLbUSVv74U7\_55vpQM0fuRhJ7khTbZioN-wBp32Zyy\_phgMi5s0qV351PoCzpZ7ueQwbsS6kvABCj2PjoeQL2trqrjcfkPfLPUksETgkVrgvi jt55bzKmUG624fv1zJbgSt7t3rrPiVQyKflW0YJcx-39sKD1CQeEFpQp\_7gnf7LoKKVPAISDLSSCHJro6R5Vm74INsQQjGn-fH55R2sS4GVw74DfWF1k7wp9Upw3Jj1gQ9MhRpVjUd98CprL-jjdna4k4CuHxZPXEoXEfkvC8PO4HmDN1Od-3ShVrilhJ1gLFpuM1814OylUju9bhHEM8R28Yl7ftgWvtzhMkdw3BPM05Uzo29xAsS\_GZeDikFl db2E7CoZu3evhnrmSk9KGbbrxcAZDFR1zhNjhBFVPpjpxgoxy6Br3LATBnu217Zt5mfAF08h EG0baz-MS0hPahefoE3S7c5xPcV4wTmmX\_r9pE\_eg-6tyiy1j5I9hOpGUmtogAgRSNA8VP5YLvoDv5D3eMhK\_ZzTQtQGEQulpA86uPKjImusrAe4XAbFE fWIPZ--S6xkYacgCzGjqfAQOIInmRLg\_fOcmuy2atMbCX9RF66rbGhOTwIY-HEBUAeIA9cY\_AL-rb78ErzcKhRodnAN3XXq\_rpA9709UjBiFm\_SEPGEsA6HlmxDopFFubEt1g-

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	<p>سازمان امور ملیان گلزار</p>
--	--	--------------------------------

36CxG41OLaKSEAXPUm105xNWUHS\_xOaT55mq4DgaX\_3cn8q6za9729x3PiGwtw0LhhH-  
sezEb7wkSW0HjJoXkRKAMKD\_HcaV7cAcwiMEvvE3sX\_JQ.m0uVEEEqSLHJRbG-xLoSyA

تکه کد زیر به زبان جاوا با در اختیار داشتن فایل کلید خصوصی امضا و گواهی امضا مودی و همچنین کلید عمومی سرور و شناسه‌ی آن کلید، از روی صورتحساب داده شده، بسته‌ی امضاشده و رمزشده را تولید می‌نماید:

```
/** Loading Signature Private Key in PKCS#8 format */
String privateKeyPath = "path/to/private-key.pem";
KeyFactory keyFactory = KeyFactory.getInstance("RSA");
final PEMParser pemParser = new PEMParser(new FileReader(privateKeyPath));
final PrivateKeyInfo pemKeyPair = (PrivateKeyInfo) pemParser.readObject();
final byte[] encoded = pemKeyPair.getEncoded();
PrivateKey privateKey = keyFactory.generatePrivate(new
PKCS8EncodedKeySpec(encoded));

/** Loading Certificate */
String certificatePath = "path/to/certificate.crt";
CertificateFactory certificateFactory =
CertificateFactory.getInstance("X.509");
X509Certificate certificate = (X509Certificate)
certificateFactory.generateCertificate(new
FileInputStream(certificatePath));

/** Loading server Key - Taken from server-information */
String serverPublicKeyString = "...[Server public key in Base64
Format]...";
String serverPublicKeyId = "...[Server Encryption Key Id]...";
final byte[] byteKey = Base64.getDecoder().decode(serverPublicKeyString);
final X509EncodedKeySpec X509publicKey = new X509EncodedKeySpec(byteKey);
final KeyFactory kf = KeyFactory.getInstance("RSA");
PublicKey publicKey = kf.generatePublic(X509publicKey);

String signatureTime = "2023-05-13T15:32:01Z";

String invoiceJson = "{ INVOICE JSON }";

/** Sign Invoice */
final JsonWebSignature jws = new JsonWebSignature();

jws.setPayload(invoiceJson);
jws.setAlgorithmHeaderValue(AlgorithmIdentifiers.RSA_USING_SHA256);
jws.setKey(privateKey);
jws.setCertificateChainHeaderValue(certificate);
jws.setHeader("sigT", signatureTime);
jws.setHeader("crit", new String[]{"sigT"});

jws.sign();

String signedJson = jws.getCompactSerialization();
```

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	<p>سازمان امور ملیان اکثر</p>
--	--	-------------------------------

```
/** Encrypt Signed Json */
final JsonWebEncryption jwe = new JsonWebEncryption();

jwe.setAlgorithmHeaderValue(KeyManagementAlgorithmIdentifiers.RSA_OAEP_256);
jwe.setEncryptionMethodHeaderParameter(ContentEncryptionAlgorithmIdentifier.AES_256_GCM);
jwe.setPayload(signedJson);
jwe.setKey(publicKey);
jwe.setKeyIdHeaderValue(serverPublicKeyId);

String encryptedInvoice = jwe.getCompactSerialization();
System.out.println(encryptedInvoice);
```

توجه کنید که این موارد به طور کامل در SDK پیاده‌سازی شده‌اند و تنها با فراخوانی یک تابع می‌توان از آن استفاده نمود. تکه کد ارائه شده صرفاً به منظور آشنايی دقیق‌تر با فرآيند تولید بسته‌ی امضاشده و رمزشده‌ی صورتحساب می‌باشد. در اين بخش هم برای عملیات تولید JWS و JWE از کتابخانه jose-4j نسخه‌ی ۰.۹.۳ استفاده شده است. همچنین تکه کد زیر به زبان .NET. همین عملیات را پیاده‌سازی می‌کند:

```
namespace TaxCollectData.Sample;

using System.Globalization;
using System.Security.Cryptography;
using System.Text.Json;
using System.Text.Json.Nodes;
using JWT.Algorithms;
using JWT.Builder;
using Org.BouncyCastle.Crypto.Parameters;
using Org.BouncyCastle.OpenSsl;
using Org.BouncyCastle.Security;
using Jose;
using Org.BouncyCastle.Utilities.Encoders;

internal class InvoiceSignAndEncryptionTest
{
    public static void Main(string[] args)
    {
        // Loading Signature Private Key in PKCS#8 format
        var privateKeyPemReader = new PemReader(File.OpenText("path/to/private-key.pem"));
        var privateKey = DotNetUtilities.ToRSA((RsaPrivateCrtKeyParameters) privateKeyPemReader.ReadObject());

        // Loading Certificate
        var certPemReader = new PemReader(new StreamReader("path/to/certificate.crt"));
        var certificate =
            DotNetUtilities.ToX509Certificate((Org.BouncyCastle.X509.X509Certificate) certPemReader.ReadObject());
        var publicKey = DotNetUtilities.ToRSA((RsaKeyParameters) DotNetUtilities.FromX509Certificate(certificate).GetPublicKey());
```

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امور ملیان گلزار</p>
--	---	--------------------------------

```

var invoiceJson = "{ INVOICE JSON }";

// Generating JWS
var signedJson = JwtBuilder.Create()
    .WithAlgorithm(new RS256Algorithm(publicKey, privateKey))
    .AddHeader(HeaderName.X5C, new []
{ Convert.ToBase64String(certificate.GetRawCertData()) })
    .AddHeader("sigT", DateTime.UtcNow.ToString("yyyy-MM-
dd'T'HH:mm:ss'Z'", CultureInfo.InvariantCulture))
    .AddHeader("crit", new [] {"sigT"})
    .Encode(JsonSerializer.Deserialize<JsonNode>(invoiceJson));

// Encrypt jws
var serverPublicKeyString = "...[Server public key in Base64
Format]...";
var serverPublicKeyId = "...[Server Encryption Key Id]...";
var decoded = Base64.Decode(serverPublicKeyString);
var asymmetricKeyParameter = PublicKeyFactory.CreateKey(decoded);
var rsaParams = DotNetUtilities.ToRSAParameters((RsaKeyParameters)
asymmetricKeyParameter);
var rsa = RSA.Create();
rsa.ImportParameters(rsaParams);
var header = new Dictionary<string, object>
{
    {
        "kid", serverPublicKeyId
    }
};
var recipient = new JweRecipient(JweAlgorithm.RSA_OAEP_256, rsa,
header);
var encryptedInvoice = JWE.Encrypt(signedJson, new [] {recipient},
JweEncryption.A256GCM, mode: SerializationMode.Compact);

Console.WriteLine(encryptedInvoice);
}
}

```

این کد نیز از همان پکیج‌های قبلی برای امضا و رمزگاری صورتحساب استفاده می‌نماید:

```

<PackageReference Include="jose-jwt" Version="4.1.0" />
<PackageReference Include="JWT" Version="10.0.2" />
<PackageReference Include="System.Security.Cryptography.Cng"
Version="6.0.0-preview.4.21253.7" />
<PackageReference Include="System.Security.Cryptography.X509Certificates"
Version="4.3.2" />
<PackageReference Include="Portable.BouncyCastle" Version="1.9.0" />

```

## ۷-۱-۴ - ارسال صورتحساب

ارسال صورتحساب از طریق فراخوانی این API به شیوه‌ی POST امکان پذیر است و از طریق آن می‌توان لیستی از صورتحساب‌ها را با هم ارسال نمود. نحوه‌ی کار این API به صورت زیر است:

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امور مالیاتی کشور</p>
---	---	---------------------------------

<b>ارسال صورتحساب – Send Invoices</b>	
https://tp.tax.gov.ir/requestsmanager/api/v2/invoice	<b>آدرس</b>
POST	<b>Method</b>
لیستی از InvoicePacket ها هر یک شامل موارد زیر:	
<ul style="list-style-type: none"> <li>• آبجکت :header</li> <li>○ uuid: شناسه منحصر به فرد درخواست از نوع requestTraceId</li> <li>○ fiscalId: از نوع رشته، شناسه حافظه صادر کننده صورتحساب</li> <li>• payload: از نوع رشته، بسته‌ی JWE صورتحساب (امضا شده و رمز شده)</li> </ul> <p>محل قرارگیری: Request Body</p> <p>در یک درخواست ارسال صورتحساب امکان ارسال حداقل ۱۰۰۰ صورتحساب وجود دارد.</p>	<b>ورودی</b>
آبجکت Json دارای فیلد های زیر:	
<ul style="list-style-type: none"> <li>• timestamp: برچسب زمانی لحظه ایجاد جواب</li> <li>• result: آرایه‌ی Json هر یک شامل شیئی که دارای فیلد های زیر است:</li> <li>○ uid: همان requestTraceId ارسال شده به ازای هر صورتحساب</li> <li>○ packetType: در اینجا null است.</li> <li>○ referenceNumber: شماره پیگیری صورتحساب ارسالی</li> <li>○ data: در اینجا null است.</li> </ul>	<b>خروجی</b>

با استفاده از این API شرکت معتمد می‌تواند همه‌ی صورتحساب‌های مودیان مختلفی که دسترسی ارسال صورتحساب را به شرکت معتمد واگذار کرده‌اند ارسال نماید و نیازی نیست همه‌ی صورتحساب‌های موجود در یک درخواست متعلق به یک شناسه یکتاً حافظه مالیاتی باشد. همچنین مودی می‌تواند در یک درخواست ارسال صورتحساب، صورتحساب‌های مربوط به شناسه یکتاها مختلف خود را ارسال نماید. البته شناسه یکتاها‌ی که اجازه‌ی ارسال صورتحساب از طریق آن‌ها را به شرکت معتمد واگذار نکرده باشد.

همچنین توجه نمایید که مقدار فیلد requestTraceId برای هر صورتحساب در یک درخواست باید منحصر به فرد باشد و در صورتی که در یک درخواست دو صورتحساب دارای requestTraceId یکسان باشند درخواست در همان ابتدا با خطأ مواجه می‌شود. همچنین در صورتی که ارسال کننده درخواست برای یک شناسه

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امور ملی اینترنت</p>
---	---	--------------------------------

یکتا برای دو صورتحساب از requestTraceId تکراری استفاده نماید هنگام استعلام وضعیت صورتحساب با uid تنها پاسخ وضعیت یکی از آنها به عنوان جواب برگردانده می‌شود.

نمونه درخواست URL ارسال صورتحساب و پاسخ آن:

```
curl -X 'POST' \
'https://tp.tax.gov.ir/requestsmanager/api/v2/invoice' \
-H 'accept: */*' \
-H 'Authorization: Bearer eyJhbGci [ JWT Token ] dLcdPeI_9Q' \
-H 'Content-Type: application/json' \
-d '[
{
  "payload": "eyJhbGciOiJ...[ JWE ]...EEzZe9mxIxw",
  "header": {
    "requestTraceId": "cf019c26-f235-11ed-a05b-0242ac120003",
    "fiscalId": "A11216"
  }
}]'
```

در صورت صحت توکن و درست بودن ساختار درخواست خروجی برابر است با:

```
{
  "timestamp": 1684054900556,
  "result": [
    {
      "uid": "cf019c26-f235-11ed-a05b-0242ac120003",
      "packetType": null,
      "referenceNumber": "3645b684-2c1e-400c-8584-f739c09d99fb",
      "data": null
    }
  ]
}
```

## - ۸ - استعلام وضعیت صورتحساب‌های ارسالی

پس از تولید یک بسته صورتحساب امضاشده و رمزشده و ارسال آن از طریق API به سرور، وب سرویس جمع‌آوری به شما یک شماره پیگیری می‌دهد و از طریق آن (یا از طریق شناسه درخواست تولیدشده توسط خودتان) و یا از طریق زمان ارسال صورتحساب می‌توانید نسبت به وضعیت پردازش صورتحساب و خطاهای احتمالی موجود در آن مطلع شوید. جزئیات خطاهای وب سرویس جمع‌آوری و لایه محتوا، در سند کدخطاهای سامانه مودیان آورده شده است. به عنوان مثال فرض کنید خروجی درخواست ارسال دو صورتحساب

به شکل زیر می‌باشد:

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امور ملی اینترنت</p>
---	---	--------------------------------

```
{
  "timestamp": 1684073047333,
  "result": [
    {
      "uid": "c5352f85-9322-41bc-a5b2-9abb130fe622",
      "packetType": null,
      "referenceNumber": "f9173085-2316-4ca6-918e-e41aaf7ef8dd",
      "data": null
    },
    {
      "uid": "2b982bfd-9a60-47cd-9da7-30fc0dabd37d",
      "packetType": null,
      "referenceNumber": "93367b02-23dd-4568-90e1-2b47d799f361",
      "data": null
    }
  ]
}
```

برای استعلام وضعیت صورتحساب سه روش وجود دارد که در ادامه شرح داده می‌شوند.

## ۱-۸ - استعلام صورتحساب به وسیله شماره پیگیری

به وسیله‌ی این API می‌توان وضعیت صورتحساب ارسالی را با استفاده از کد پیگیری‌ای که وب سرویس جمع آوری به ازای هر صورتحساب در اختیار قرار می‌دهد استعلام نمائیم. نحوه‌ی کار این API به صورت زیر است:

- استعلام به وسیله شماره پیگیری - Inquiry by Reference Id	
آدرس	Method
<p><a href="https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-reference-id">https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-reference-id</a></p> <p>فیلدهای زیر:</p> <ul style="list-style-type: none"> <li>referenceIds: لیست شماره‌ی پیگیری‌هایی که قرار است استعلام شوند.</li> <li>start: شروع بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T00:00:00.000000000+03:30</li> <li>end: پایان بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T23:59:59.123456789+03:30</li> </ul> <p>ورودی‌های start و end اختیاری هستند و در صورتی که مقدار دهی نشوند، جستجو در بین صورتحساب‌های ارسالی در ۲۴ ساعت گذشته انجام می‌گیرد. همچنین بازه زمانی مورد استعلام نمی‌تواند از یک هفته بیشتر باشد.</p> <p>محل قرار گیری: Request Params</p>	<b>ورودی</b>

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	<p>سازمان امور ملی ایمنی و کنترل</p>
---	--	--------------------------------------

آرایه‌ی JSON شامل اشیائی با محتویات زیر (به ازای هر شماره پیگیری یک شیء JSON در این آرایه برگردانده می‌شود):

- referenceNumber: شماره پیگیری درخواست استعلام شده
- uid: شناسه درخواست (همان requestTraceId که صورتحساب با آن ارسال شده بود)
- status: وضعیت صورتحساب دارای حالت‌های زیر:
  - SUCCESS: صورتحساب فاقد خطا بود و با موفقیت در کارپوشه ثبت شد.
  - FAILED: صورتحساب ارسالی دارای خطا بوده و رد شده است.
  - IN\_PROGRESS: صورتحساب ارسالی هنوز در صفحه بررسی می‌باشد.
  - NOT\_FOUND: شماره پیگیری داده شده یافت نشد.
- data: لیست خطاهای موجود در صورتحساب
- packetType: نوع بسته
- fiscalId: شناسه حافظه ارسال‌کننده صورتحساب
- sign: امضا پاسخ به فرمت بسته JWS که ساختار آن در جدول بعدی توضیح داده می‌شود (فقط در حالت SUCCESS)

### خروجی

همانطور که گفته شد خروجی درخواست استعلام صورتحساب دارای فیلدی به نام sign می‌باشد که این فیلد در حالت SUCCESS مقدار دهی شده و در سایر حالات برابر با "" می‌باشد. ساختار این فیلد JWS که توسط هسته تولید و مقداردهی می‌شود به شکل زیر است:

امضا پاسخ نتیجه‌ی اعتبارسنجی صورتحساب – JWS	
یک شیء JSON دارای فیلدهای زیر:	
alg: الگوریتم امضا: RS256	Header
sigT: زمان امضا توکن	Payload

Format: yyyy-MM-dd'T'HH:mm:ss'Z'  
Example: 2023-05-13T10:44:47Z

شیء JSON دارای فیلدهای زیر:  
referenceNumber: شماره پیگیری درخواست صورتحساب ارسالی. مثال:

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	 <p>سازمان امور مالیاتی کشور</p>
---	--	---

6e1c7696-064c-4d95-b9eb-711ab931a734

• شناسه‌ی فرستنده‌ی صورتحساب. مثال: clientId

A1112K

• شماره مالیاتی صورتحساب موفق درج شده در کارپوشه. مثال: taxId

A1112K04D1271489087018

• تاریخ دریافت صورتحساب در سامانه مودیان. مثال: receivedDate

2024-01-08T11:38:54.388Z

امضای بسته‌ی حاصل از الحاق Header و Payload با استفاده از الگوریتم RS256 و با استفاده از کلید سازمان.

شما می‌توانید صحت امضا بسته را با استفاده از کلید عمومی سازمان (دریافتی از متدهای Get) اعتبارسنجی نمایید.

**Signature**

نمونه داده‌ی امضا شده هنگام استعلام وضعیت صورتحساب:

```
eyJhbGciOiJSUzI1NiIsInPz1QiOiiyMDI0LTayLTE0VDAzOjA4OjM5WiJ9.eyJyZWz1cmVuY2V0dWlizXIIoiIzMTk3NzhLMC03Zjg0LTQyNDktOThmNC1kZTc5OTBjYjdjNjkiLCJjbG1lbnRJZCI6IkExMTFPSyIsInRheElkijoiQTExMU9LMDREMzYxMjAwRThEQjIxNCIsInJlY2VpdmVkJRGF0ZSI6IjIwMjQtMDITMTNUMTE6NTI6NDIuOTgyWiJ9.lan1052gttnAp6F1MX9NxPn9swN4
-
IjFiowTX2ytm_1YgAqgzBLytvTBRrq_NopeIH9LIRD275iFJaysMxbFmVnstTLp91hG_iMGFFQvAXxwY5EL_LYnexus-
bIPSSwftXK91f6RjKrIIDm0hyBr2pCZpc_ZXSgwLHyaf1p_GgxvYSql413xCNzzFKfp3yI8r0Pa
hIHovmUlkbcdriH_YXKckDw9Z1H6a3NcVs1mj65Ed7pemBMmJLPf_Kj7tn7e8s4dUGH0fs6HEotY
fCB7LMDejPDu6jgbIPkwANHWAx3dZoE03bUKSo6SiYInvo3GQvDP5dpvGngkQ9NAme7HKg-
HjDHJJzEcjKACG-
Gj3LEsyQveHrL4s5q9YGYWwavZVinbTRMw175_LRgTeB1UuWNVLS5PtSk2o6drzRnNJ6iN542HH
tOvnF_y8J57o01LHXDtMS5ncQF2e_NJ2tGmFxQs868T1ODgqaHzBc3H7VyQ8KC1uD_W3zAf93e
1ErKbAdVt2eDHZVFHoREZVoYW3m7qra05fiYcYUle9TUXLARQwd_ihEcKbRtLbtw42ZHqfxZe52
Q77vJdY79Xb80kUjA5kfJ6g4o80Qqa-NaIoeWrFte0g5e-
SUSJk1nd4pZTTApZfCMOnoKFSGJ0USfi0T3M-OX7lyxJbOYKeqUzt4
```

نمونه درخواست استعلام وضعیت صورتحساب با استفاده از شماره پیگیری:

```
curl -X 'GET' \
  'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-reference-id?referenceIds=f9173085-2316-4ca6-918e-e41aaf7ef8dd&referenceIds=93367b02-23dd-4568-90e1-2b47d799f361&start=2023-05-14T10%3A00%3A00.00000000%2B03%3A30&end=2023-05-14T21%3A00%3A00.00000000%2B03%3A30' \
  -H 'accept: */*' \
  -H 'Authorization: Bearer eyJhbGciO...[ JWT TOKEN ]...q4RcXogA'
```

در صورت صحت توکن و درست بودن ساختار درخواست خروجی برابر است با:

```
[
  {
    "referenceNumber": "93367b02-23dd-4568-90e1-2b47d799f361",
```

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	<p>سازمان امور ملیان اکثر</p>
--	--	-------------------------------

```

"uid": "2b982bfd-9a60-47cd-9da7-30fc0dabd37d",
"status": "FAILED",
"data": {
  "error": [
    {
      "code": "012802",
      "message": "فیلد در شده وارد مقدار "مجاز مقادیر جز «تسویه روش» فیلد در شده وارد مقدار "نیست",
      "errorType": "ERROR"
    }
  ],
  "warning": [],
  "success": false
},
"packetType": "receive_invoice_confirm",
"fiscalId": "A111OK",
"sign": ""
},
{
  "referenceNumber": "f9173085-2316-4ca6-918e-e41aaf7ef8dd",
  "uid": "c5352f85-9322-41bc-a5b2-9abb130fe622",
  "status": "SUCCESS",
  "data": {
    "error": [],
    "warning": [],
    "success": true
  },
  "packetType": "receive_invoice_confirm",
  "fiscalId": "A111OK",
  "sign": ""
}
"eyJhbGciOiJSUzI1NiIsInPz1QiOiIyMDI0LTAYLTE0VDAzOjA40jM5WiJ9.eyJZWZlcVuY
2VOdW1izXIIoIzMTk3Nzh1MC03Zjg0LTQyNDktOThmNC1kZTc5OTBjYjdNjkiLCJjbG1lbnRJ
ZC16IkExMTFPSyIsInRheElkIjoiQTExMU9LMDREMzYxMjAwRThEQjIxNCIsInJ1Y2VpdmVkJGF
0ZSI6IjIwMjQtMDItMTNUMTE6NTI6NDIuOTgyWiJ9.lanl052gttnAp6F1MX9NxPn9swN4-
IjFiowTX2ytm_1YgAqgzBLytvTBRrq_NopeIH9LIRd275iFJaysMxbFmVnstTLp91hG_iMGFFQv
AXxwY5EL_LYnexus-
biPSswfTXK91f6RjKrIIDm0hyBr2pCZpc_ZXSgwLHyaf1p_GgxvYSq1413xCNzzFKfp3yI8r0Pa
hIHovmUlkbcdriH_YXKckDw9Z1H6a3NcVs1mj65Ed7pemBMmJLPf_Kj7tn7e8s4dUGh0fs6HEotY
fCB7LMDejPDu6jgbIPkwANHWAxx3dZoeO3bUKSo6SIyInvo3GQvDP5dpyGngkQ9NAme7HKg-
HjDHJJzEcjKACG-
Gj3LEsyQveHrL4s5q9YGYWwavZVinbTRMwl75_LRgIeB1UuWNVLs5PtSk2o6drzRnNJ6iN542HH
tOvnF_y8J57o1LHXDtpMS5ncQF2e_NJ2tGmFxQs868T1ODgqaHzBc3H7Vq8KC1uD_W3zAf93e
1ErKbAdVt2eDHZVFHoREZVoYW3m7qraO5fiYcYule9TUXLARQwd_ihEcKbRtLbtw42ZHqfxZe52
Q77vJdY79Xb8OkUjA5kfJ6g4o80Qqa-NaIoewrFte0g5e-
SUSJklnd4pZTTApZfCMOnoKFSGJ0USfi0T3M-OX7lyxJbOYKeqUzt4"
}
]

```

همانطور که می‌بینید یکی از صورتحساب‌ها با موفقیت ثبت شده و هیچ خطأ و اخطاری ندارد. ولی یکی از صورتحساب‌ها دارای خطأ بوده و خطأ موجود در آن در قسمت error قابل مشاهده می‌باشد.

## ۸-۲-۸ استعلام با uid

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	<p>سازمان امور ملی اینترنت</p>
---	--	--------------------------------

فراخوانی این API دقیقا همانند استعلام به وسیله Reference number است با این تفاوت که در ورودی به جای شماره پیگیری، uid و fiscalId می‌گیرد.

استعلام به وسیله شناسه درخواست – Inquiry by uid	
آدرس	Method
<a href="https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-uid">https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-uid</a>	GET
فیلدهای زیر:	
<ul style="list-style-type: none"> <li>uidList: لیست شناسه درخواست‌های صورتحساب‌های مورد نظر</li> <li>fiscalId: شناسه حافظه صادر کننده صورتحساب</li> <li>start: شروع بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T00:00:00.000000000+03:30</li> <li>end: پایان بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T23:59:59.123456789+03:30</li> </ul>	ورودی
ورودی‌های start و end اختیاری هستند و در صورتی که مقدار دهی نشوند، جستجو در بین صورتحساب‌های ارسالی در <u>۲۴ ساعت</u> گذشته انجام می‌گیرد.	
Request Params:	محل قرارگیری:
دقیقا مانند استعلام با شماره پیگیری	خروجی

نمونه درخواست و پاسخ این API را می‌توانید ببینید:

```
curl -X 'GET' \
  'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-
uid?uidList=cb080c58-e36f-4bb0-a932-90f672109fb6&uidList=b3bd6327-1c57-
4cae-85ed-5c88de28aea3&fiscalId=A111YO&start=2023-06-
10T00%3A00%3A00.000000000%2B03%3A30&end=2023-06-
10T23%3A59%3A59.999999999%2B03%3A30' \
-H 'accept: */*' \
-H 'Authorization: Bearer eyJhbGciOiJ...[JWT TOKEN]...1kvski8e-A'
```

در صورت صحت توکن و درست بودن ساختار درخواست خروجی برابر است با:

```
[{"referenceNumber": "780c7cb1-84cf-4df8-a87d-160448f38c55",
"uid": "b3bd6327-1c57-4cae-85ed-5c88de28aea3",
"status": "FAILED",
"data": {
  "error": [
    {
      "code": "E001"
    }
  ]
}]]
```

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	<p>سازمان امور ملی اینترنت</p>
--	--	--------------------------------

```

    "code": "011107",
    "message": "شناسه/ملی شناسه/شماره» فیلد در شده وارد مقدار طول",
    "errorType": "ERROR"
  },
  ],
  "warning": [
    {
      "code": "111208",
      "message": "خریدار اقتصادی شماره» فیلد در شده وارد مقدار طول",
      "errorType": "WARNING"
    }
  ],
  "success": false
},
"packetType": "receive_invoice_confirm",
"fiscalId": "A111OK",
"sign": ""
},
{
  "referenceNumber": "60e834f9-14b6-43be-8b77-85471678d3da",
  "uid": "cb080c58-e36f-4bb0-a932-90f672109fb6",
  "status": "SUCCESS",
  "data": {
    "error": [],
    "warning": [],
    "success": true
  },
  "packetType": "receive_invoice_confirm",
  "fiscalId": "A111OK",
  "sign": "
"eyJhbGciOiJSUzI1NiIsInNpZ1QiOiiyMDI0LTAYLTERvDEyOjAxOjExWiJ9.eyJyZWZlcmVuY
2V0dW1iZXIIoIjMmWQyMDYwZC0zMzzkLTQwNDUTYjg2ZC03ZTAwMTUzOWQyZTUiLCJjbG1lbnRJ
ZC16IkExMTFPSyIsInRheElkIjoiQTExMU9LMDREMzY3MjJEMzk2QzQ2MyIsInJ1Y2VpdmvkRGF
0ZSI6IjIwMjQtMDITMTNUMTI6MDE6MDcuODk0WiJ9.PK1MMmv1U6aVsB4u6CvVD4UANik5QFmlot
tsnil9EwOjEBTLpn_2S0bkBN5CecIGDX7abRMr8X3H385_gE1og1Cv_F7e-
_r5JVzQVbks82AFhUGkT09AGjhTqTQk45MvtOY1mb26YgsWovERP4ApgINLUwJH9Pw4otnorHI
eNgnu-_JKTVPul4mnfTFMeb7PTDUyy9uIbpwaR5BbVL8OPTL6J4RA151I-coTLnCUMi9LLj-
rUDVkhjdf3_NPL7NADA4GvZwgFZ3Fv2sZxete8z7DBuN4ZdNhvpbs9fYlqdwEkoTE2ZsgD9XapE
1UMDCQt8oAGG4G2W0JInb30F2ZrSqq2UaVSZ3OicZFBj8qXoGlX7IomcgCJ2Bs991c4umrn78Mx
2s2UFiF9ckkfJgsIUgpk3jeQ8oEVJuLCRoeTA5MmP4j3Z_z2AFDzkazhZAXmGfDtp6O80HHKz4K
pm77ccTgIPiIYZawb5VUZe1OdOdgub2T2q3aeP7bA91ue4ntmYaL19vjaEhi7XI5XdbH189t7x
20aHx_DR70h2KI9hbFZBSEZJM_JmXPDJ6s1hFvHcb1MPf-
p9ft2r3Noj5mNiBUREnTLi6NvUXwUz6hhspvdE-xrW51aMkGPp4_Zy51YNKi9KZ1d_EWhMpwe-
HtQjXeVEyc8ldkE4uSP6IE"
  }
]

```

همانطور که مشاهده می‌کنید، یکی از صورتحساب‌ها با موفقیت در کارپوشه ثبت شده و دیگری دارای خطای باشد و لیست خطاهای و هشدارهای موجود در صورتحساب برگردانده می‌شوند.

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امور ملیان گنثور</p>
---	---	--------------------------------

### ۸-۳- استعلام براساس بازه‌ی زمانی

این API نیز مانند دو مورد قبلی است و صورتحساب‌های فرستاده شده در یک بازه‌ی زمانی مشخص را به صورت صفحه‌بندی شده برمی‌گرداند. همچنین امکان فیلتر کردن صورتحساب براساس وضعیت نیز وجود دارد.

<b>استعلام در بازه زمانی Inquiry</b>	
<a href="https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry">https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry</a>	<b>آدرس</b>
GET	<b>Method</b>
فیلدهای زیر:	
<ul style="list-style-type: none"> <li>• <code>pageNumber</code>: شماره صفحه (مقدار پیشفرض: ۱)</li> <li>• <code>pageSize</code>: اندازه صفحه (مقدار پیشفرض: ۱۰ - مقادیر مجاز: ۱ تا ۱۰۰)</li> <li>• <code>status</code>: وضعیت صورتحساب‌هایی که به دنبال آن هستیم.</li> <li>○ مقادیر مجاز: SUCCESS, FAILED, TIMEOUT, IN_PROGRESS</li> <li>○ در صورتی که این فیلد خالی باشد همه‌ی صورتحساب‌ها برگردانده می‌شود.</li> <li>• <code>start</code>: شروع بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T00:00:00.000000000+03:30</li> <li>• <code>end</code>: پایان بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T23:59:59.123456789+03:30</li> </ul>	<b>ورودی</b>
ورودی‌های <code>start</code> و <code>end</code> اختیاری هستند و در صورتی که مقدار دهی نشوند، جستجو در بین صورتحساب‌های ارسالی در <u>۲۴ ساعت</u> گذشته انجام می‌گیرد.	
Request Params	
دقیقاً همانند استعلام با شماره پیگیری و <code>uid</code>	<b>خروجی</b>

نمونه درخواست ارسالی:

```
curl -X 'GET' \
  'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry?start=2023-06-10T00%3A00%3A00.000000000%2B03%3A30&end=2023-06-10T23%3A59%3A59.999999999%2B03%3A30&pageNumber=1&pageSize=10' \
  -H 'accept: */*' \
  -H 'Authorization: Bearer eyJhbGciOi...[JWT TOKEN]...iKKXzBjRZw'
```

در صورت صحت توکن و درست بودن ساختار درخواست خروجی برابر است با:

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	 <p>سازمان امور ملیان کمک ثور</p>
--	--	--

```
[
  {
    "referenceNumber": "780c7cb1-84cf-4df8-a87d-160448f38c55",
    "uid": "b3bd6327-1c57-4cae-85ed-5c88de28aea3",
    "status": "FAILED",
    "data": {
      "error": [
        {
          "code": "011107",
          "message": "شناسه/ملی شناسه/شماره» فیلد در شده وارد مقدار طول «خریدار فرایگیر کد/مدنی مشارکت مقدار طول). است مجاز طول حد اکثر از بزرگتر (باشد 10 حد اکثر باید شده وارد
          "errorType": "ERROR"
        }
      ],
      "warning": [
        {
          "code": "111208",
          "message": "«خریدار اقتصادی شماره» فیلد در شده وارد مقدار طول «(باشد 14 حد اقل باید شده وارد مقدار طول). است مجاز طول حد اقل از کوچکتر
          "errorType": "WARNING"
        }
      ],
      "success": false
    },
    "packetType": "receive_invoice_confirm",
    "fiscalId": "A111OK",
    "sign": ""
  },
  {
    "referenceNumber": "60e834f9-14b6-43be-8b77-85471678d3da",
    "uid": "cb080c58-e36f-4bb0-a932-90f672109fb6",
    "status": "SUCCESS",
    "data": {
      "error": [],
      "warning": [],
      "success": true
    },
    "packetType": "receive_invoice_confirm",
    "fiscalId": "A111OK",
    "sign": "eyJhbGciOiJSUzI1NiIsInNpZ1QiOiIyMDI0LTAYLTE3VDA5OjA3OjUzWiJ9.eyJyZWZlcmVuY2V0dWlizXIIoii4MjczYzhkMiljNWJmLTQyYmQtYTQwZi0wNDA1MjA5YzU2MjkiLCJjbG11bnRJZC16IkExMTFPSyIsInRheElkIjoiOTEwMU9LMDREM0FFQjM1MjAxQTc1NyIsInJ1Y2VpdmVkJcIjIwMjQtMDItMTdUMDk6MDc6NTEuNDUyWiJ9.VnC48sJLngr2YqjpD50bHYmBP0oIZP-KK7CxB9aZjTPAU5x4xKSyYdCNGRfW1LmnHRpVAHUKs3oeRsHF_uxFD2nGDC6qXHg6MFOcnLU3HcIETk-tqIgyVRv3eO6zMyf9ImjatQkD-niW0wjyk7YkK_wl3XFy71ve4YMnR2yE49V-1ejjj1CwlhICyV1MKG-IkpNfNy76HA3V0mPZ7Jt1b2cSFt037WVkd9eAGMSl8biQYXsPHgsulf1USHIrqAWCGaqQfkp_qFC2nHC4um8RXGAKfxqBQTbmvSEOEk7R3dxRsciNSsxseS9QZIDJqMPmxZcOZFjT0H5Gt8Kpgj2qj3LcVxXyk3R_QGH1w8FhLU8SAECCnLtkPazz8I_WHnSAowXvV_N3gKB5QkCLK-8No2LPvkttsuDT1R5-GB8wi2cTsxsRug9QI0MCKBvbGVntsR5oEA_UgP-pT7OMXswFsvkoCAmkEfRaqr0-IFzNU6z2NVy8bNZ4snwp8VaQNbqXgxuncUVikdoUsbC_uT648alg6QZw4xDeRCbt29Ut9VNY91sUT9s5BCnyS1B-
```

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	 <p>سازمان امور مالیاتی کشور</p>
---	---	---

```
6fk4IhQUO8KkpD37HMTCTNHur33dFQ_qDHG4zcttGI1Q4lj7f6FwP8c1wW59oVCAJfLyekJjGr5
a0aqJtQXF3G5YwBzfQmtRj6hP62cyWC5ixv8"
}
]
```

## استعلام اطلاعات حافظه و مودی - ۹

### - ۱- اطلاعات حافظه

این API اطلاعات مربوط به حافظه مالیاتی (شامل فعال بودن / عدم فعال بودن، حد مجاز فروش و شماره اقتصادی متصل به آن) را بر می گرداند. نحوه کار این API به صورت زیر است:

دریافت اطلاعات حافظه - GET Fiscal Information		
آدرس	Method	
<a href="https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information">https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information</a>	GET	
• <b>memoryId</b> : شناسه حافظه مورد نظر • <b>nameTrade</b> : شناسه حافظه • <b>fiscalStatus</b> : وضعیت حافظه • <b>nationalId</b> : شناسه ملی پرونده / کد ملی صاحب پرونده • <b>economicCode</b> : کد اقتصادی پرونده	<b>ورودی</b> <b>Request Params</b>	
شیء JSON شامل فیلدهای زیر: • <b>nameTrade</b> : شناسه حافظه • <b>fiscalStatus</b> : وضعیت حافظه • <b>nationalId</b> : شناسه ملی پرونده / کد ملی صاحب پرونده • <b>economicCode</b> : کد اقتصادی پرونده		<b>خروجی</b>

نمونه ورودی:

```
curl -X 'GET' \
'https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-
information?memoryId=A11216' \
-H 'accept: */*' \
-H 'Authorization: Bearer eyJhbGc...[ JWT Token ]...OFh9zw'
```

در صورت صحت توکن و درست بودن ساختار درخواست خروجی برابر است با:

```
{
    "nameTrade": "A11216",
    "fiscalStatus": "ACTIVE",
    "nationalId": "14003778990",
    "economicCode": "14003778990"
}
```

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سنده دستورالعمل فنی اتصال به سامانه مودیان</b></p>	<p>سازمان امور مالیاتی کشور</p>
---	--	---------------------------------

## ۹-۲-۱- اطلاعات مودی

این API اطلاعات پرونده مودی را بر می گرداند و نحوه کار آن به شکل زیر است:

دریافت اطلاعات مودی - GET Taxpayer		آدرس Method
<a href="https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer">https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer</a>	GET	
Request Params	economicCode: شماره اقتصادی مودی nameTrade: نام مودی / پرونده اقتصادی taxpayerStatus: وضعیت پرونده شامل فیلدهای NOT_ALLOCATED و DEACTIVATED به معنی غیرفعال nationalId: شناسه ملی پرونده / کد ملی صاحب پرونده	ورودی
شیء JSON شامل فیلدهای زیر: ▪ nameTrade: نام مودی / پرونده اقتصادی ▪ taxpayerStatus: وضعیت پرونده شامل فیلدهای NOT_ALLOCATED و DEACTIVATED به معنی غیرفعال ▪ nationalId: شناسه ملی پرونده / کد ملی صاحب پرونده	خروجی	

نمونه درخواست ارسالی:

```
curl -X 'GET' \
'https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer?economicCode=1400377
8990' \
-H 'accept: */*' \
-H 'Authorization: Bearer eyJhbGci...[ JWT Token ]...klQXOM-_uA'
```

در صورت صحت توکن و درست بودن ساختار درخواست خروجی برابر است با:

```
{
  "nameTrade": "انزلی آزاد منطقه ایرانیان الکترونیک پیشخوان",
  "taxpayerStatus": "ACTIVE",
  "nationalId": "14003778990"
}
```

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امور ملیان گنثور</p>
---	---	--------------------------------

## ۱۰- استعلام وضعیت صورتحساب در کارپوشه

این سرویس وضعیت صورتحساب ها را بر میگرداند و نحوه کار آن به شکل زیر است.

<b>استعلام وضعیت صورتحساب – GET INVOICE STATUS</b>		
آدرس	Method	ورودی
<a href="https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-invoice-status">https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-invoice-status</a>	GET	
شیء JSON شامل فیلدهای زیر:		
▪ شماره مالیاتی صورتحساب :taxIds		Request Params
▪ محل قرارگیری: invoiceStatus		
▪ مقدادیر زیر: article6Status		
▪ خطای مقدادیر زیر: error		
خروجی		
REJECTED(رد شده)		
APPROVED(تایید شده)		
SYSTEMIC_APPROVED(تایید سیستمی)		
IMPOSSIBLEREACTION(عدم امکان واکنش)		
AWAITINGREACTION(در انتظار واکنش)		
NO_NEEDREACTION(عدم نیاز به واکنش)		
CANCELED(باطل شده)		
▪ مقدادیر زیر: article6Status		
▪ خطای مقدادیر زیر: error		
EXCEEDED(عدول)		
NOT_EXCEEDED(عدم عدول)		
▪ مقدادیر زیر: error		
NOT_FOUND(صورتحساب یافت نشد)		
ACCESS_DENIED(دسترسی ندارید)		

نمونه درخواست ارسالی:

```
curl -X 'GET' \
'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-invoice-
status?taxIds=A111DW04E8300004349008&taxIds=A111DW04E8300003CC4EA5' \
```

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	<p>سازمان امور مالیاتی کشور</p>
---	---	---------------------------------

```
-H 'accept: */*' \
-H 'Authorization: Bearer eyJhbGci...[ JWT Token ]...klQXOM-_uA'
```

در صورت صحت توکن و درست بودن ساختار درخواست خروجی برابر است با:

```
[ {
  "taxId": "A111DW04E8300004349008",
  "invoiceStatus": "APPROVED",
  "article6Status": "NOT_EXCEEDED",
  "error": null
},
{
  "taxId": "A111DW04E8300003CC4EA5",
  "invoiceStatus": "APPROVED",
  "article6Status": "NOT_EXCEEDED",
  "error": null
}]
```

## ۱۱- ارسال پرداخت صورتحساب

این وب سرویس بدین صورت است که مودی می‌تواند با فراخوانی سرویس پرداخت تجمیعی صورتحساب مرتبط با مورد کاربرد برای صورتحساب‌های الکترونیکی که روش تسویه آنها به صورت نسیه یا نقدی/نسیه هستند ثبت پرداخت انجام دهد و وضعیت پرداخت انجام شده را به صورت همگام مشاهده کند.

آدرس Method	
<a href="https://tp.tax.gov.ir/requestsmanager/api/v2/invoice-payment">https://tp.tax.gov.ir/requestsmanager/api/v2/invoice-payment</a>	POST

Request Body: شی ارسال پرداخت paymentRequest

- محل قرارگیری: Request Body
- Json شامل فیلدهای زیر است

ورودی
(شماره مالیاتی صورتحساب) taxid
(مبلغ پرداخت) paidAmount
(تاریخ و زمان پرداخت) paymentDate

<p>شناسه سند</p> <p>RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	<p>سازمان امور ملیا و کشور</p>
--	--	--------------------------------

<p>(روش پرداخت) paymentMethod •</p> <ul style="list-style-type: none"> <li>▪ چک : CHEQUE</li> <li>▪ تهاتر : BARTER</li> <li>▪ وجه نقد : CASH</li> <li>▪ دستگاه پوز : POS</li> <li>▪ درگاه پرداختی اینترنتی : INTERNET</li> <li>▪ کارت به کارت : CARD</li> <li>▪ انتقال به حساب : TRANSFER</li> <li>▪ دیگر : OTHER</li> </ul> <p>(شماره پایانه) terminalNumber •</p> <p>(شماره مرجع پرداخت) referenceNumber •</p> <p>شامل موارد زیر میباشد PaymentMethod</p>	<p>شيء JSON شامل فیلدهای زیر:</p> <p>▪ وضعیت درخواست requestStatus •</p> <p>▪ شامل (SUCCESS, FAILED)</p> <p>▪ لیست خطاهای شامل error •</p> <ul style="list-style-type: none"> <li>○ کد خطا (code)</li> <li>○ پیغام خطا (Message)</li> </ul> <p style="text-align: right;">خروجی</p>
---	---

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h1>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h1>	 <p>سازمان امور ملیان کشور</p>
---	--	---

نمونه درخواست ارسالی:

```
curl -X GET 'https://tp.tax.gov.ir/requestsmanager/api/v2/ /invoice-payment' \
-H 'accept: */*' \
-H 'Authorization: Bearer eyJjcm10Ij...-w' \
-H 'Content-Type: application/json' \
-d '{
  "taxId": "A111H104EA6001D0B32AC6",
  "paidAmount": 0,
  "paymentDate": 0,
  "paymentMethod": "CHEQUE",
  "terminalNumber": "string",
  "referenceNumber": "string"
}'
```

در صورت صحت توکن و درست بودن ساختار درخواست خروجی برابر است با:

```
{
[
  "requestStatus": "SUCCESS",
  "error": [
    {
      "code": "string",
      "message": "string"
    }
  ]
}
```

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<p><b>سند «دستورالعمل فنی اتصال به سامانه مودیان»</b></p>	 <p>سازمان امور مالیاتی کشور</p>
---	---	---

## ۱۲- پیوست‌ها

### ۱- گواهی و کلید خصوصی امضا

گواهی امضایی که در Header بسته‌های JWS فرستاده می‌شود برابر است با:

```
-----BEGIN CERTIFICATE-----
MIIDejCCAmmKgAwIBAgIUV27QXqJjk2EgFy9zeYkpsX+ISPsWQYJKoZIhvcNAQEL
BQAwcTELMAkGA1UEBhMCSVIXDDAKBgNVBAgMA1R1aDEMMAoGA1UEBwwDVGVoMREw
DwYDVQQKDAhNb2hheW1lbjEMMAoGA1UECwwDVGf4MSUwIwYJKoZIhvcNAQkBFhZt
Lm1hbHZlcmRpQG1vaGF5bWVuLmlYMB4XDTIzMDMyNDEzMjgyM1oXDTI0MDMyMzEz
MjgyM1owTTEPMA0GA1UEAwwGQW56YWxpMRcwFQYDVQQKDA5RdW9WYWRpcyBHcm91
cDELMAkGA1UEBhMCSVIXFDASBgnVBAUTCzE0MDAzNzc40TkwmIIBIjANBhkqhkIG
9w0BAQEFAAOCAQ8AMIIIBCgKCAQEazLgyk5K06+j9d1ud0i1JArrZ3Whw/w9wEzHB
9yXwENRa5fm5AbRukMF5b6VGeKzD6LZuL9+tfdfFfWyPcjI++gGNy wzRmEHKpTnzP
1t6NyuxKfm4nBVAb1sugSw8Y5DEXRFTqILgBWN/pZ4zGlifEALMcGAs7ADcjnv7b
/tM2wxr9rHxsCvW4Hv1zQasK8Qr1CrKgT0E166rSXCHep/uIONDwp0W20e1m1ZtM
6AAjWXRLGcshPIHuK+ZLFAFxWtoGonf6qN9ypos2B18D/EFa8WHON62eYKT0kW3j
BVa3yPEkRwdkDjDu/3CPzymhf3WFYwxb4t35oWb/qUXGVIdvwIDAQABoy4wLDAf
BgNVHSMEGDAwBGSx+Oq+RO3x/FmyCp+jcmfOH+Fn9TAJBgnVHRMEAjAAMA0GCSqG
SIb3DQEBCwUA4IBAQAgKATXlnS+pPtAiRIYGtydVU5Vi7Aq+D6QW07uFqcB7vBh
ddN3yX21VVcwpTNJzhv8UCM+mDMvlmsRVKVtMoo5fHfII92/Wo8rUz1RP+yhyCk0
Vz8I11v+bjLwVur/agC/s5Rf0m66pNNjFZ9J3S2N31ChXYwz2vvA8pdAYvWTu9g5
u4FMFqlsaLwMGC+WaA0g3KYzRkdWRY1vd23hLTUcVsWM8wpgZ11wEGE1khca/Sd0
mCU2HG5vIbqFFtJA6to0fy07CE5fD8aR3UcXjNduosV052ZqCX5SabrhFS3AGHFR
jpFnI5LZespiCXSAs8Sv3k0SCSRQKqFbiwSFM8Zjg
-----END CERTIFICATE-----
```

همچنین کلید خصوصی متناظر با این گواهی که در فرآیند امضای بسته‌ها استفاده شده کلید زیر است:

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggsjAgEAAoIBAQDMuDKTko7r6P13
W53SKUkCutndaHD/D3ATMcH3JfA01Fr1+bkBtG6QwX1vpUZ4rMPotm4v36190V9b
I9yMj76AY3LDNGYQcq10fM/W3o3K5cp+bicFUBuWy6BLDxjkMRdF90oguAFY3+ln
jMaWJ8QAsxwYCzsANy0e/tv+0zbDGv2sfGwK9bge+XNBqwrxCvUKsqBPQQjrqtJc
Id6n+4g40NanRbY56UyVm0zoACNZdEsZyyE8ge4r5kt8AXFa2gaid/qo33KmizYH
XwP8QVrxYc43rZ5gpPSRbeMFVrfI8SRHCR0OM07/cI/PKaF/dYVjDGlvi3fmhZv+
pRcZUh2/AgMBAAECggEACPpC7YnNzram9ucDosXAt+ftyfHckrLgnVbfRLFbN8G4
QsGSxWpeNub1Jmo/Due0p63oYx0SBKR75AlMkLV1CzhRPhI8L5h3qEN88dVMrosp
OCYoe+kpbJF9dA0zcD5e40h+o/StynH3UF0yED+qLsWsA7nqWnYQj9ZpW2Fz01Z1
i5NRX4YgyIopHfqcLWJWp0R8n4HwDY18BL7tMi31f0sZXz56EUgBPxq5RMi+1iKW
-----END PRIVATE KEY-----
```

<p>شناسه سند RC_TICS.IS_v1.5</p> <p>اردیبهشت ۱۴۰۴</p>	<h2>سند «دستورالعمل فنی اتصال به سامانه مودیان»</h2>	<p>سازمان امور ملیا و کشور</p>
---	--	--------------------------------

pyZdwy4TrJL/Sj4tWkKJ7ELVd47VunizAqeLDy8bL1PBX0PewRvR37P9axHLjsj/  
d1Iw/xvqgVEWZTyUXzg4qgFU5Na5u6xIW8JyqejdEQKBgQD2Q1DdoP0tG1URyuuo  
4HJ1Q85ZfEWWA0vvp8esvJLJ7t73Rz28RkKAMHW/njr23ExxV3eek9J1lGENJUZF  
KsNNtjRWMgCxUic00MGTJuraWHrEma00YNNjpVd3pIi68p51CZNzMRLn2J8F+7CP  
eGiynKEvKU43KcJr6K0kWP14FQKBgQDU0T3SNr7af4y3r03ds2DMaoKEG531tuLu  
nrZNnL4a/i2r3AlI5K470UkmAXDD1kgGf235KxrRm7x7Vvp5SZLg0PqgJ2OKKk9b  
HLvuAdxCeUlnDfJWrAmYcmYLCSDHBDuN/evF6WiNaQi074MhdbaxYdLiiXds3VV  
f1Q/8m6/gwKBgD4ijXTeX52V/+j1YnDB8RtL+IzrpkMrocVeeCtFiwQaOXf7KcCP  
mcfuckdfDVGsVD1k7HG+qq0wRKykcw6Qs6awCpSVGUekiuZaFf2jHC7r1E522BUX  
OT8zQNaXVUiWxxT4zzOLF1IZfkZsMyiAISqwCptzuKCCkOPZVzDoo0vhAoGBAMo8  
2XnVyoKLKwc2r4i600eo48S1FeP12yuVqXqr1FqEZ1R1MnGR1z1DAjdasRV5oVKD  
cDeTzdWZIE3uFWAJFJt80WUiNQ4ptbXtINWQ0DsT2PebggNTsUPH7UVytDJ0jiq  
gfZjC2TdgtAR1g3Cdk3J3mtbqeX1GmiXN2rZcIMPAoGADfTonaehrsnsCucH4Dgs  
qZdyZm9JRmoNyisLBmbGkTNxoY09Vm/03u3NMsohkjopt2ly38ZMYX14FyXKEKcI  
977r33JD9PxRcovqFhcPR3WuQrPf6ND3IX6eB5p8d7m6fmFYSe/0NhwoeH99a6/c  
csAr2hPMOb/R3GdRewkSGgQ=  
-----END PRIVATE KEY-----