



سازمان امور مالیاتی کشور

مرکز تنظیم مقررات نظام پایانه‌های فروشگاهی و سامانه مودیان


سند

«دستورالعمل فنی اتصال به سامانه مودیان»

شناسه سند:

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

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 وب سرویس می‌باشد که تمامی درخواست‌ها از طریق این وب سرویس به سامانه ارسال شده و پاسخ داده می‌شوند. این وب سرویس در چهارچوب REST API پیاده سازی شده و فراخوانی آن نیازمند احراز هویت^۱ مودی از طریق امضای دیجیتال می‌باشد.

در این سند منابع موجود در این وب سرویس و نحوه‌ی فراخوانی و پاسخ دهی هر کدام شرح داده خواهد شد و در نهایت در قالب یک مثال فرآیند اتصال به سامانه‌ی مودیان و ارسال صورتحساب به طور کامل انجام می‌گیرد.

تغییرات این سند نسبت به نسخه‌ی قبلی


ردیف	عنوان تغییر	بخش مرتبط
۱	اضافه شدن سرویس استعلام وضعیت صورتحساب در کارپوشه	بخش ۱۰

^۱ Authentication

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

فهرست مطالب

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


شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

۱ - تعاریف

عنوان	تعریف
امضای دیجیتال ^۲	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.
گواهی امضا ^۳	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 امضای بسته‌های ارسالی مورد استفاده قرار می‌گیرد.
صورتحساب الکترونیک	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.
شماره مالیاتی	شماره منحصر به فرد مشخص‌کننده یک صورتحساب شامل شناسه حافظه مالیاتی صادرکننده صورتحساب، تاریخ صدور، سریال صورتحساب و یک رقم کنترلی برای جلوگیری از صدور شماره مالیاتی‌های نامعتبر.
شناسه یکتای حافظه مالیاتی	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.

Digital Signature^۲

Digital Signature Certificate^۳

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

۲ - دریافت شناسه یکتای 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:

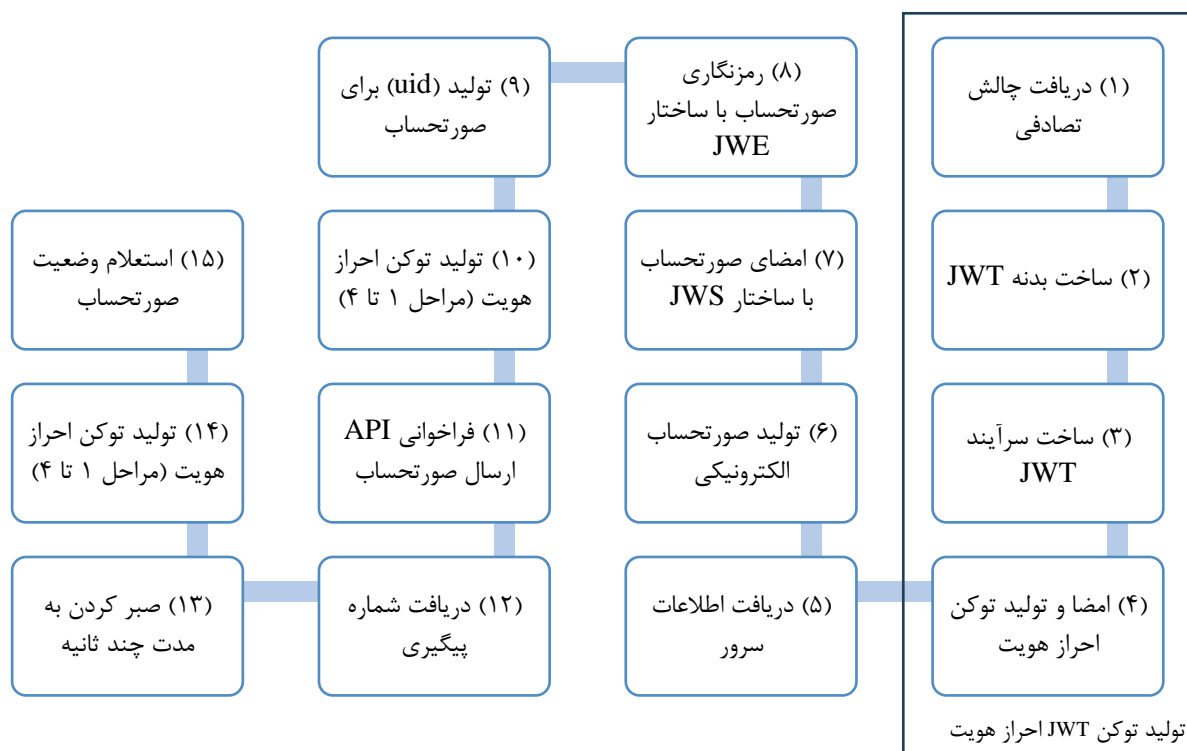
۱. به ازای هر شناسه یکتا حافظه مالیاتی، یکی از سه حالت ارسال اطلاعات صورتحساب را به شرح ذیل انتخاب کند:

- 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 API های 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 API های سامانه مودیان نیز فراهم می‌باشد که راهنمای استفاده از آن به پیوست این سند بارگذاری گردیده است.

۳ - مراحل ارسال صورتحساب و استعلام وضعیت آن




۴ - منابع در دسترس و کاربردهای هر کدام

وب سرویس جمع آوری 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 فراخوانی همه‌ی منابع موجود در وب سرویس جمع آوری سامانه‌ی مودیان نیازمند احراز هویت فراخوانی 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.

آدرس	درخواست	ساختار خروجی	توضیحات
GET https://tp.tax.gov.ir/requestsmanager/api/v2/nonce	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/nonce?timeToLive=20' \ -H 'accept: */*'</pre>	<pre>{ "nonce": "string", "expDate": "string" }</pre>	دریافت چالش تصادفی راهنما در صفحه ۱۰
POST https://tp.tax.gov.ir/requestsmanager/api/v2/invoice	<pre>curl -X 'POST' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/invoice' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGc [JWT Token] dLcdPeI_9Q' \ -H 'Content-Type: application/json' \ -d '[{ "payload": "eyJhbGciOiJ...[JWE]...EEZze9mxIiw", "header": { "requestTraceId": "cf019c26-f235-11ed-a05b-0242ac120003", "fiscalId": "A11216" } }]'</pre>	<pre>{ "timestamp": 0, "result": [{ "uid": "string", "packetType": "string", "referenceNumber": "string", "data": "string" }] }</pre>	ارسال صورتحساب راهنما در صفحه ۱۸
GET https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer?economicCode=14003778990' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbG...[JWT Token]...k1QXOuA'</pre>	<pre>{ "nameTrade": "string", "taxpayerStatus": "string", "nationalId": "string" }</pre>	دریافت اطلاعات پرونده‌ی مودی راهنما در صفحه ۴۳
GET https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information	<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>	<pre>{ "nameTrade": "string", "fiscalStatus": "string", "nationalId": "string", "economicCode": "string" }</pre>	دریافت اطلاعات حافظه راهنما در صفحه ۴۲
GET https://tp.tax.gov.ir/requestsmanager/api/v2/server-information	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/server-information' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGci...[JWT]...Jv18fvHm0PKVA'</pre>	<pre>{ "serverTime": 0, "publicKeys": [{ "key": "string", "id": "string", "algorithm": "string", "purpose": 0 }] }</pre>	دریافت اطلاعات سرور راهنما در صفحه ۱۷

استعلام صورتحساب با شماره پیگیری راهنما در صفحه ۳۴	<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&referenceIds=93367b02-23dd-4568-90e1-2b47d799f361&start=2023-05-14T10%3A00%3A00.000000000%2B03%3A30&end=2023-05-14T21%3A00%3A00.000000000%2B03%3A30' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGc...[JWT TOKEN]...q4RcXogA'</pre>	GET https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-reference-id
استعلام با شناسه درخواست (uid) راهنما در صفحه ۳۷	<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&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 eyJhbGciO...[JWT TOKEN]...ski8e-A'</pre>	GET https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-uid
استعلام براساس بازه زمانی راهنما در صفحه ۴۰	<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=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 eyJhbGci...[JWT TOKEN]...KXzBjRZw'</pre>	GET https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry
استعلام وضعیت صورتحساب در کارپوشه راهنما در صفحه ۴۴	<pre>[{ "taxId": "A111DW04E8300004349008", "invoiceStatus": "APPROVED", "article6Status": "NOT_EXCEEDED", "error": null }, { "taxId": "A111DW04E8300003CC4EA5", "invoiceStatus": "APPROVED", "article6Status": "NOT_EXCEEDED", "error": null }]</pre>	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-invoice-status?taxIds=A111DW04E8300004349008&taxIds=A111DW04E8300003CC4EA5' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGci...[JWT Token]...k1QXOM-_uA'</pre>	GET https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-invoice-status

جدول ۱

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

۵ - دریافت چالش تصادفی و احراز هویت

مکانیزم احراز هویت در وب سرویس جمع آوری 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 باشید.

۵-۱ - 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^۴ (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. فراخوانی درخواست بعدی با قرار دادن توکن در سرآیند درخواست

فرآیند احراز هویت بدین صورت است که ابتدا شما باید API چالش تصادفی را فراخوانی 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.

^۴ Nonce

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

۵-۱-۱ 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	https://tp.tax.gov.ir/requestsmanager/api/v2/nonce
Method	GET
ورودی	<ul style="list-style-type: none"> timeToLive: مدت زمان اعتبار رشته تصادفی به ثانیه <ul style="list-style-type: none"> نوع ورودی: اختیاری محل قرارگیری: Request Params مقدار پیش فرض: ۳۰ مقادیر مجاز: ۱۰ تا ۲۰۰
خروجی	<ul style="list-style-type: none"> nonce: رشته تصادفی تولید شده expDate: زمان انقضای رشته تصادفی

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 امضای Nonce و تولید توکن


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

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

ساختار توکن JWS		
Header	<p>یک شیء JSON دارای فیلدهای زیر:</p> <ul style="list-style-type: none"> alg: الگوریتم امضا: RS256 x5c: لیستی که شامل گواهی امضای مودی باشد. کد شده به فرمت Base64 sigT: زمان امضای توکن <p>○ فرمت:</p> <p>yyyy-MM-dd'T'HH:mm:ss'Z'</p> <p>○ نمونه:</p> <p>2023-05-13T10:44:47Z</p> <ul style="list-style-type: none"> crit: لیستی از فیلدهای ضروری در قسمت Header. تنها شامل رشتهی "sigT" 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: <p>2023-05-13T14:14:47Z+0330</p> <p>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.</p> 	
	<p>یک شیء Json دارای دو فیلد زیر:</p> <ul style="list-style-type: none"> nonce: رشته تصادفی یکبارمصرف دریافت شده clientId: شناسه ارسال کننده صورتحساب <p>○ برای مودیان همان شناسه حافظه صادر کننده صورتحساب</p> <p>○ برای شرکت‌های معتمد شناسه شرکت معتمد</p>	Payload
<p>ورودی الگوریتم امضا برابر است با:</p> <p>ASCII (BASE64URL (UTF8 (JWS Protected Header)) '.' BASE64URL (JWS Payload))</p>		Signature

شناسه سند	<p>سند «دستور العمل فنی اتصال به سامانه مودیان»</p>	 <p>سازمان امور مالیاتی کشور</p>
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

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

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

```

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` بارگزاری 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-4` 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;

```

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

```
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.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>(payload));

        Console.WriteLine(jws);
    }
}
```

این کد از پکیج‌های زیر برای امضای بسته 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" />
```

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

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

حال باید با استفاده از این توکن هنگام ارائه درخواست بعدی خود را به سرور معرفی نمائیم. بدین منظور باید در سرآیند درخواست HTTP ارسالی، فیلد Authorization را برابر با "Bearer [jwt token]" قرار دهیم. مثلاً 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 eyJhbGciOi....'
```

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 خطا در هر بخش صحت امضای بسته زیر سوال می‌رود و توکن فرستاده شده مورد قبول واقع نمی‌شود:

۱. ساختار کلی بسته‌ی JWS (payload 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.

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

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) استعمال 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 استعمال 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 برمی‌گرداند. همانطور که گفته شد فراخوانی این API نیاز به احراز هویت دارد و جهت فراخوانی آن باید توکن JWT در قسمت header درخواست در فیلد Authorization فرستاده شود. نحوه‌ی کار این API به صورت زیر است:

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

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

○ key: کلید کد شده به فرمت Base64	
○ id: شناسه کلید	
○ algorithm: فعلا 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]...Jv18fvHm0PKVA'
```

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

```
{
  "serverTime": 1684055518885,
  "publicKeys": [
    {
      "key":
      "MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAXdzREOEfK3vBQogDPGTMqdDQ7t0oDh
      uKMZkA+Wm1lhzzjHAGfSUOuDVOKRoUEQwP8oUcXRmYzcvCUgcfoRT5iz7HbovgH+bIeJwT4rmLm
      FcbfPke+E3DLUXOtIZifEXrKXWgSVPkRnhMgym6UiAtznwA1rmKstJoWpk9Nv34CYgTk8DKQN5j
      QJqb9L/Ng0zOEEtI3zA424tsd9zv/kP4/SaSnbbnj0evqsZ29X6aBypvnTnWH9t3gbWM4I9eAVQ
      hPYClawHTqvdaZ/O/feqfm06QBFnCGl+CBdjLs30xQSLsPICjnlV1jMzoTznAabWP6FRzzj6C2s
      xw9a/Ww1XrKn3gldZ7Ctv6Jso72cEeCeUIltzHMDJPU3Qy12RQzaXuJpMhCz1Dva47RvqiumpTN
      yK9HfFIdhgoupFkxT14XLD165S55MF6HuQvo/RHSbBJ93FQ+2/x/Q2MNGB3BXOjNwM2pj3oJbDv
      3pj9CHzvaYQUYMlyOcFmIJqJ72uvVf9Jx9iTObaNNF6p152ADmh85GTAH1hz+4pR/E9IAXUI1/Y
      iUneYu0G4tiDY4ZXyKYNknNfhSgxmn/gPHT+7kL3lnyxgjIEEhK0B0vagWvdRCNJSNGWpLtlq4F
      lCWTAnPI5ctiFgq925e+sySjNaORCoHraBXNEwyiHT2hu5ZipIW2cCAwEAAQ==",
      "id": "6a2bcd88-a871-4245-a393-2843eafe6e02",
      "algorithm": "RSA",
      "purpose": 1
    }
  ]
}
```

۷ – ارسال صورتحساب

فرآیند ارسال صورتحساب هم مانند تمامی فرآیندها در وب سرویس جمع آوری نیاز به احراز هویت فراخوانی کننده دارد. بنابراین از تکرار این مرحله صرف نظر می کنیم. فرض می کنیم عملیات گرفتن nonce، امضای آن و ساخت توکن برای هر درخواست انجام می شود. فرض کنید یک صورتحساب الکترونیک در اختیار داریم. برای آشنایی با صورتحساب الکترونیکی و فیلدهای آن به سند [«دستورالعمل صدور صورتحساب](#)

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

الکترونیکی مراجعه نمائید. 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 نمائیم. سپس باید صورتحساب را امضا کنیم و بسته ی JWS تولید نمائیم. در مرحله ی بعدی باید از صورتحساب امضا شده، به وسیله کلید عمومی سازمان (که از طریق GET server-information دریافت می گردد) بسته ی رمز شده ی JWE ساخته شود و سپس برای وب سرویس جمع آوری ارسال شود.

۷-۱- جزئیات فرآیند ارسال صورتحساب


۷-۱-۱- تولید شماره ی 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 نرم افزاری (SDK) به زبان های جاوا و net. توابعی جهت تولید شماره مالیاتی مطابق با الگوریتم های گفته شده پیاده سازی شده که نحوه ی استفاده از آن ها شرح داده خواهد شد.

۷-۱-۲- امضای صورتحساب

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

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

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		


توجه کنید که بررسی اعتبار امضا و گواهی امضا کننده‌ی صورتحساب نیز عیناً همانند بررسی توکن JWS می‌باشد و در کنار بررسی گواهی امضای صادرکننده‌ی صورتحساب و تاریخ انقضای گواهی، از سرور OCSP و CRL صادرکننده‌ی 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 معتبر بوده و کد ملی/شناسه ملی موجود در گواهی^۷ دسترسی ارسال صورتحساب برای شناسه یکتای 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 باز کردن و مشاهده محتویات صورتحساب را نداشته باشد. الگوریتم رمزگذاری مورد استفاده در این مرحله AES256-GCM (AES/GCM/NoPadding) می‌باشد و کلید AES نیز از طریق الگوریتم RSA-OAEP-256 (RSA-OAEP using SHA-256 and MGF1 with) RSAES OAEP using SHA-256 and MGF1 with) 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 رمز شده 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 رمز شده 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 وب سرویس سامانه‌ی مودیان ارسال نمود.

^۷ فیلد SERIALNUMBER در قسمت SUBJECT گواهی امضاء

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

ساختار شیء JWE:


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

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

<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)
```


شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

مراحل رمز گذاری صورت حساب:

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 می شود:

```
eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIiwia2lkIjoiaNmEyYmNkODgtYTg3MS00MjQ1LWEzOTMtMjg0M2VhZmU2ZTAyIn0
```

توجه کنید که رشته ی سرآیند (header) حتما باید به فرمت utf-8 باشد.

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

```
_hm__fdwWlcK2FiFuuOHcRHqvKeYrd9_tzAdUI9IK5E
```

سپس این کلید را با کلید عمومی رمز گذاری سامانه مودیان به طول ۴۰۹۶ بیت، رمز می کنیم. این کلید از API


دریافت اطلاعات سرور دریافت می شود و مقدار آن به فرمت Base64 برابر است با:

```
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAXdzREOEfk3vBQogDPGTMqdDQ7t0oDhuKMZkA+Wm1lhzzjHAGfSUOuDVOKRoUEQwP8oUcXRmYzcvCUgcfoRT5iz7HbovqH+bIeJwT4rmLmFcbfPke+E3DLUxOtIZifEXrKXWgSVPkRnhMgym6UiAtnzWAlrmKstJoWpk9Nv34CYgTk8DKQN5jQJqb9L/Ng0zOEETI3zA424tsd9zv/kP4/SaSnbbnj0evqsZ29X6aBypvnTnwH9t3gbWM4I9eAVQhPYClawHTqvdaZ/O/feqfm06QBFnCGl+CBdjLs30xQSLsPICjnlV1jMzoTznAabWP6FRzzj6C2sxw9a/WwlXrKn3gldZ7Ctv6Jso72cEeCeUI1tzHMDJPU3Qy12RQzaXujpMhCzlDva47RvqiumpTNYK9HfFidhgoupFkxT14XLD165S55MF6HuQvo/RHSbBJ93FQ+2/x/Q2MNGB3BXOjNwM2pj3ojbDv3pj9CHzvaYQUYm1yOcFmIJqJ72uvVf9Jx9iTObaNNF6p152ADmh85GTAH1hz+4pR/E9IAXUI1/YiUneYu0G4tiDY4ZXYkYNknNfhSgxmn/gPHT+7kL31nyxgjiEEhK0B0vagWvdRCNJSNGWpLtlq4F1CWTAnPI5ctiFgq925e+sySjNaORCoHraBXNEwyiHT2hu5ZipIW2cCAwEAAQ==
```

و حاصل رمز شده ی کلید متقارن با کلید عمومی به فرمت Base64URL سازمان می شود. قابل توجه است که

خروجی رمز شده الگوریتم ۲۵۶-RSA-OAEP با ورودهای یکسان، متفاوت خواهد بود:

```
1Rs_vcZlauJs4VwED3wZGr3wJDdbg8It9zBStuJgqf7TiGs3kUCSulPwA6jRA-8xuHTpNtKrlw0hsNbUhsx-3BL5zGaDzsSekAlAZVevVy2qOrfId6OxLOb81SpVnSRR_K3jRHDWfH_ZDgZqMoM2mv6qFvb8GgGFV59_jIkhtX73Y6iqe3NCask2CT0Ine3SUFVxt_OBqnBCwgDLrauGyisQbpVN1JJRjsWPeyXA00Wv1ECnRSLs93-prnMrfLTU_JHUYU304-cq7gVu7OATP1NB78L8m0-MiIF_tr0mpbaEneOLDbimNYt2UVgn1thJsvh5Na30GKY5t-ISHoWhX-DvVHp3KTEpp0bkc8IczZt-jg-2vdYhyM7Sz1H0c9w2EvSSryYsAVonOojl4yWeaNHp_7mk09hgu1MUkr91Tfr-U1k3zFHyCClfJzHj3t3uebS2mFDEyuao7K4omC335_VYsCi6kRSU421AW1_8V21RxaS2VDBQbgoCqr3UQXssoSRIG3v1-OBgTgZ9slEGZnEihaptab-7IeqnXIbhZNA8Onzy0wKW2S6r8M2eDd01QhGaDPGXcdWtOpC-Q-
```


شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

cvu9MJTp4MRDx5dYe2rRQaI_A7WS5vJGkjwdRRpfhaJhGoXA7Wc6eUmB_UFOvPfsGQdFXPBUB3v
h6jPfsER6hnXjU

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 AAD (Additional Authenticated Data) داریم که مقدار آن از طریق محاسبه مقدار ASCII سرآیند (Header) Encode شده به فرمت Base64URL به دست می آید:


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

Base64URL(Header): eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIiwia2lkIjoianNmEyYmNkODgtYTg3MS00MjQ1LWEzOTMtMjg0M2VhZmU2ZTAyIn0


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-
5XdZfdIMlR4ghYPDT_rfE0GjmroEaWOaoM3qXwDhdUFs1nb_48KAUOQY1ebgd9Ngi_ed-
rh517TAj1wPCmqnPEY9SYIPeorurSwlMPPpI9NN-bjjBUhWla4RxkCt5UeHDS--
bvRkPqD5DaiOQg2RD7n8cm6pzHKcKO16WpXSSFhIjK1-
l_kevoprXPIEHtWik3PBSXYWDz15Gc_ET-aw2CF6xgWkUi-
vw512_ySvs66grxGqubBQkOOxLLyUEmcxedPSCSs6g4eNqf-
SES0yZ9NR4uBs3WBSqs2h0Ftrn5ZKniMDQKtoU0LJvscjXBso6ckAVuvjBilY4zKgr07FjJ9zn-
9xkStotxms0czBo-
fOsVunTuKypLBvTiwV4uykqUnsxbyOtuUvr10kLK1dma4F9q1gixRqfoMynlo7seRDTRrTkBh_D
krF-
AzNhZG3o1TC5bHUtwn5crc2dw3FkS4UMelunQkusFL44MRqY3qbn_iP4NY8X3bWTWtp3lkiFxFkT
ATTiZG_lvi5omlQwCA7a_mYQw47EjjvGTiSJQsfdM8d2WB1VD0V65xgcqy7OQVRPxfTo6jJu-
X1MGd-RN2Lb_crLsnJGJ6kpdhgyF7ts_3gbWvryzKLJyDe2HM3izN6Kw0U4Ba-__YOMPV-
mJECsVC5KUw9jRYhw6tdYSU41LXKRDnMyh-

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

cjRyuv4V347DOR280aGWSbqpqaDp4mdtkaABARhtO5BhbzzeSnHnEjTVZmdn8H5WifzGvqHCiGA
z752CNNO00OwCbpVoW2Jcq78XndubsxsXzkcq0XvsDxnKzdBdRkoYyTEd5tModxUZw_tpbXNQZF
FwAB4ph_FtoYC0j5OkGhEola6h7jguoFJu0CewloGSkvvqu2Ht4G9IfDkFs0tMTvdjHJJGWpDj9
nQ_Mzn0QkKBPhGLM50yUtosIVd1FvrHCJuhkt3qsAP60THvgDswELnLMcOsoRB2qdVp6YSAOT3Z
uRc6Bawwd5S78wd_o4ISW9pNMxNbHPueiXI_N48S9Zcb2ktwH6dB3rbkRwgXCEWcPheX8s5ik32
5PbY5RAs29fj45yISSZ-
6xlg9BwBXjg81TkNg18_6j0aI8ZZmDjL1EyjK0ojb9UpQUfjreakNAGhxSa5S_ethmI63Bs6_En
XyzOKDP5sPmlyBgJ6RjXRSmVI8zqA1ETazPY93PYql_PqADQm48_Ocs1h_djjNNBHeA8ucYelX1
T8tcD-ENwrvJw8_2ulA1DWX-
FucPGQQLZc4Pkw04OCUeBlxDUsJFzedhX0cKEQr_b9zxhVT3C09yr3q6FyhqrYF892Kql06PmXB
VEZrb-Q0piVZyozeordNJGRE016r8A10hnc-KgUlkDZrxee_zzk9aV08CU01-
fvBRGGR12v_EAcY17pnyfnCKmZH3u3Iq5D7-
T3JHJSZz2NuUFRcok81L87X0YbRCscW164VAEsF1QolakktKt8cNRQwj_95rttlKa06FdG6Q-
VK9NskncKRKnLwCIQT6Ec6eTmr1Ng7JaQ7dqkEh_zThM8ifE-
Ak6jVdpMiHZ4Nvd1OndCPbilr7zFNrUeRI0BK5PWFOJA90YAnMJ3B7DkrAMyLhZMkKXp4UjEZSQ
hBhe_lnd9VxL3rZcmRqEctFVmsTnyRZY-
pZlSx8gS__99WXrtNqD1lR3njeHWJScI35GoJJwWh3BFCJvsyeQcmsIkkN4RdBrwj_B-
ZpUKJn1gvho2E7PPkvuMpMPSWr1clzptCpzamAY2pTjBgmQ5NWDnxN87fUZN9YaJYMcqD7kb-
kooJuNWw7TcF-YPo_31UHHwd3mKzBVfUeYEqqJBA-
9KromQzfc7hc5QQkaA_oGVn0_8_AexX7fNDdXc6yRzM_msfGsbO6pMYegbEijS5F3DaopvpAmwd
BbFlDRUIGSKpfODn9DNGB2BoqNnlmNPCu_BsqGuPvF3RzgxP-1MoCI3Xf7RxG1DYr-
bTPsV6pyzinV5HaGSNRorYkXchaXhl19k4d9pfu_4uXeASFVG6WxzdpVwb_w769VQdVYL7KG0u4
uC_MhWDH0w1DVEFySffBNPpZ6Z_1LYkbc8epocBH9HjJVfByP4gqVieVuDlX_tkK6QUwSPZTl36
Be4uVf9luAJXZfn3IkMbJ8KuRfLjwBE3N4MnjXbz4RHN5dZwaSJftRgYo_DaJPiqcGz1H3dB5B4
i0A7bLA4H1TEIKLPom-
AlGnpRruGdoF7dD3dhx8HOKUt7ny7zMrYQWI86bmRzubnMZmi87GguvCoCP7o7ATMJIGprSDmg-
3TJ5FGyeXaNRZ0LEP1Dhc6uh19Pm_PYP7l8tKg5Z_dGgnFWwJp2SDweU7kvWgEUePJVa-
HKd7iirGP-
2cttS8ak4z1q_OjKkFRHi6A2uZ95Yg0dkWgBbHgCHbbuM5oBmIztFixmnHeoTrV3HPbBPw2jEX_
XINhFVcYnfc1efs0Gh-
jKA4wrCgStq5bXRhMC5degaoQ0Sb5eY_S_Ehpz1yoA_JYDHP6t8FfnSMTNbM9LfoBTgZDdlrRmw
d2dBVJxzkbhTpXo4dpShFRSL1vs0GV3wdELBuzMb3UaTyu-
rJy_DOb1fPE8pmlC1NS2_WhrVXB0gJf91MaaIup_Fx7tJzSbqiNG9mFj6SQvMk0HvAyI195NpyF
NX33x5NLFnF6125mZdn6MY6nLPeNu9PlyEadZ8uXnMtwfrAOuN83yS2XZDWKHPYSJOaVcsGAjRr
cGLpulp-dcx1g0XVQgNR0KzaH7J3zbRJ-Lqf7V6w9aYT1JnHk2lbof2oGp9NaWN1-
TqlOEvrAk3-
EqzyCigOG5A2YZdoRR_1rlCxfNCXz0dtRwM07IX_kEEEKHTs4lk970YTSa_SdhYNMUN0QPBLkjT
ts_YMnx8Y2wFumFy9Ji3K5o2GHB5nc0a1DioSi9gNEpFjv6pT_Tk9NDIFUBAwv8oV_qp41qFqSp
A9g6G51madn0K6sonvAsRlDWNjxSBropglstgWWCre3Ucp_b9PhZht1rSuJsZynEqLCf9ZLn21x
fugLbIodvaNZxkI2NtNHCv_CsiMfo76rC5SwCJ5uTtD64z53s2txbOPmhWpIGE63OKi3fQSZz5H
ZdBbidIRCM3vCEseMNw1A27F7_BCIN6o9tZd-1X0Zkvh08Wts2d-clFs-
x5ssLWeoMPpGvnFjZ9pQBD8EyK34JsA5qPTVjLOD62ZRph8PdkijIoE0es4QmyleVbUe9rbScIN
F2m5YSHiRWWM5MFSpDFmT67EtriseeWQnVNQTU31_chDRut92yv2G3seSa8HHMLW0Gmq7W7hUUG
uxLbUSVv74U7_55vpQM0fuRhJ7khTbZioN-
wBp32Zyy_phgMi5sOqV35lPoCzpZ7ueQwbsS6kvABCj2PjoeQL2trqrjcfkPflPUKsETgkVrgvi
jt55bzKmUG624fv1zJbgSt7t3rrPiVQyKflW0YJcx-
39sKDICQeEFpQp_7gnf7LoKKVPAISDLSSCHJro6R5Vm74INsQQjGn-
fh55R2sS4GVw74DfWF1k7wp9Upw3JjlgQ9MhRpVjUd98CprL-
jjdn4k4CuHxZPXEOXEfkvC8PO4HmDN1Od-
3ShVrilhJ1gLFpuM1814OylUju9bhHEM8R28YL7ftgWvtzhMkdW3BPM05Uzo29xAsS_GZeDikFl

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		


db2E7CoZu3evhnrMsk9KWGbbrxcAZDFR1zhNJHJBFVPPjpxgoXy6Br3LAtZBnu2l7Zt5mfAF08h
EG0baz-MS0hPahcfoE3S7c5xPcV4wTmmX_r9pE_eg-
6tyiylj5I9hOpgUMtogAgRSNA8VP5YLvDv5D3eMhK_ZzTQtQGEQulpA86uPKjImusrAe4XAbFE
fWIPZ--S6xkYacgCzGjqfAQOInmRLg_fOcmuy2atMbCX9Rf66rbGhOTwIY-HEBUAeIA9cY_AL-
rb78ErzcKhRodnAN3XXq-rpA9709UjBiFm_SEPGESa6HlmdoPFubEt1g-
36CxG41OLaKSEAXPUM105xNWUHS_xOaT55mq4DgaX_3cn8q6za9729x3PiGwtw0LhlhH-
sezEb7wkSW0HjJoXkrKAMKD_HcaV7cAcwiMEvvE3sX_JQ

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


m0uVEEEeqSLHJRbG-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:

eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIiwia2lkIjoiNmEyYmNkO
DgtYTg3MS00MjQ1LWEzOTMtMjg0M2VhZmU2ZTAyIn0.1Rs_vcZlauJs4VwED3wZGr3wJDdbg8It9
zBStuJgqf7TiGs3kUCSulPwA6jRA-8xuHTpNtKrlw0hsNbUhsx-
3BL5zGaDzsSekAlAZVevVy2qOrfId6OxLOb81SpVnSRR_K3jRHDWfH_ZDgZqMoM2mv6qFvb8GgG
FV59_jIkhtX73Y6iqe3NCask2CT0Ine3SUFVxt_OBqnBCwgDLrauGyisQbpVN1JJRjsWPeyXA0
0Wv1ECnRSLs93-prnMrfLTU_JHUYU304-cq7gVu7OATP1NB78L8m0-
MiIF_tr0mpbaEneOLDbimNYt2UVgn1thJsvh5Na30GKY5t-ISHoWhX-
DvVHp3KTEpp0bkC8IczZt-jg-
2vdYhyM7Sz1H0c9w2EvSSryYsAVonOojl4yWeaNhP_7mk09hgu1MUKr91Tfr-
U1k3zFHyCClfJzHj3t3uebS2mFDEyuao7K4omC335_VYsCi6kRSU421AW1_8V21RxaS2VDBQbgo
Cqr3UQXssoSRIG3v1-OBgTgZ9slEGZnEihaptab-
7IeqnXIbhZNA8Onzy0wKW2S6r8M2eDd01QhGaDPGXcdWtOpC-Q-
cvu9MJTp4MRDx5dYe2rRQaI_A7WS5vJGkjwdRRpfhaJhGoXA7Wc6eUmB_UFOvPfsGQdFXPBUB3v
h6jPfsER6hnXjU.75ZoCO0VRqIWRyAs.GiB15WaoRrEeK77gX1Tr-
141X0520tRcvrhp8D9cHCfYLTionEo3MXYQ46Z8QTPv2ueCdiKztQDngTuczGGY3lvelcz-
tHqeAJ92UG9cjouMVE7IY29ML7OrzPy66GJsVb3BZnmIm6vDNEMf9AL8LH3y-
H4rk9JmZjQbrRIU2AbmTGwRK0_FnQD660b-4nEMKfc51h9bk-
dc8as3_OxFH2b0KxaiZDKi8pDLumCFPQ9U9pfU7KUmKfL09FGF3FpryGX5DzEE_YprotK6lcEr9
f8U5ooHS_Pf06pprnL_CkXtimdJEnJgghk-
5XdZfdIMlR4ghYPDT_rfE0GjmroEaW0aoM3qXwDhdUFs1nb_48KAUOQY1ebgd9Ngi_ed-
rh5l7TAj1wPCmqnPEY9SYIPEorurSwlMPPpI9NN-bjjBUhWla4RxxCt5UeHDS--
bvRkPqD5DaiOQg2RD7n8cm6pzHKcK016WpXSSfHijK1-
l_kevoprXPIEHtWik3PBSXYWDz15Gc_ET-aw2CF6xgWkUi-
vw512_ySvs66grxGqubBQkO0xLLyUEmcxedPSCSs6g4eNqf-
SES0yZ9NR4uBs3WBSqs2h0Ftrn5ZKniMDQKtoU0LJvscjXBso6ckAVuvjBilY4zKgr07FjJ9zn-
9xkStotxms0czBo-
fOsVunTuKypLBvTiwV4uykqUnsxbyOtuUvrl0kLK1dma4F9q1gixRqfoMyn1o7seRDTRrTkBh_D
krF-
AzNhZG3o1TC5bHUtwn5crc2dw3FkS4UMelunQkusFL44MRqY3qbn_iP4NY8X3bWTWtp3lkiFxFkT
ATTiZG_lvi5omlQwCA7a_mYQw47EjjvGTiSJQsfDM8d2WB1VDOV65xgcqy7OQVRPxfTo6jJu-
X1MGd-RN2Lb_crLsnJGJ6kpdhgyF7ts_3gbWvryzKLJyDe2HM3izN6Kw0U4Ba-__YOMPV-
mJECsVC5KUw9jRYhw6tdYSU41LXKRdnMyh-
cjRyuv4V347DOR280aGWSbqpqaDp4mdtkaABARhtO5BhbzZeSnHnEjTVZmdn8H5WifzGvqHCiGA
z752CNNO00OwCbPvOW2Jcq78XndubsxsXzkcq0XvsDxnKzdBdRkoYyTED5tModxUzw_tpbXNQZF

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

FwAB4ph_FtoYC0j5OkGhEola6h7jguoFJu0CewloGSkvvqu2Ht4G9IfDkFs0tMTvdjHJJGWPdJ9
nQ_Mzn0QkKBPhGLM50yUtosIVd1FvrHCJuhkt3qsAP60THvgDswELnLMcOsoRB2qdVp6YSAOT3Z
uRc6Bawwd5S78wd_o4ISW9pNMxNbHPueiXI_N48S9Zcb2ktwH6dB3rbkRwgXCEWcPheX8s5ik32
5PbY5RAs29fj45yISSZ-
6xlg9BwBXjg81TkNg18_6j0aI8ZZmDjLlEyjK0ojb9UpQUfjreakNAGhxSa5S_ethmI63Bs6_En
XyzOKDP5sPmlyBgJ6RjXRSmVI8zqAlETazPY93PYq1_PqADQm48_Ocs1h_djjNNBHeA8ucYelX1
T8tcD-ENwrvJw8_2u1A1DWX-
FucPGQQLZc4Pkw04OCUEBlxDUsJFzedhX0cKEQr_b9zxhVT3C09yr3q6FyhqrYF892Kq106PmXB
VEZrb-Q0piVZyozeordNJGRE016r8A10hnc-KgUlkdZrxee_zzk9aV08CU01-
fvBRGGR12v_EAcY17pnyfnCKmZH3u3Iq5D7-
T3JHJSZz2NuUFRcok81L87X0YbRCscWl64VAESf1QolakktKt8cNRQwj_95rttlKa06Fd6gQ-
VK9NskncKRKn1WcIQTE6Ec6Tmr1Ng7JaQ7dqKEh_zThM8ife-
Ak6jVdpMiHZ4Nvd1OndCPbilr7zFNrUeRI0BK5PWfOJA90YAnMJ3B7DkrAMyLhZMkKXp4UjEZSQ
hBhe_lnd9VxL3rZcmRqEctFVmsTnyRZY-
pZlSx8gS__99WXrtNqD1lR3njeHWJScI35GoJJwWh3BFCJvsyeQcmsIkkN4RdBrwj_B-
ZpUKJn1gvho2E7PPkvuMpMPSWr1clzptCpzamAY2pTjBgmQ5NWDnxN87fUZN9YaJYMcqD7kb-
kooJuNWw7TcF-YPo_3lUHHWd3mKzBVfUeYEqqJBA-
9KromQzfc7hc5QQkaA_oGVn0_8_AexX7fNDdXc6yRzM_msfGsb06pMYegbEijS5F3DaopvpAmwd
BbFlDRUIGSKpfODn9DNGB2BoqNnlmNPCu_BsqGuPvF3RzgxP-1MoCI3Xf7RxGLDYr-
bTPsV6pyzinV5HaGSNRorYkXchaXhl19k4d9pfu_4uXeASfVG6WxzdpVwb_w769VQdVYL7KG0u4
uC_MhWDH0w1DVEFySffBNPpZ6Z_lLYkbc8epocBH9HjJVFByP4gqVieVuDLX_tkK6QUWSPZT136
Be4uVf9luAJXZfn3IkMb78KuRfLjwBE3N4MnjXbz4RHN5dZwaSJftRgYo_DaJPiqcGz1H3dB5B4
i0A7bLA4H1TEIKLPom-
AlGnpRruGdoF7dD3dhx8HOKUt7ny7zMrYQWI86bmRzubnMZmi87GguvCoCP7o7ATMJIGprSDmg-
3TJ5FGyeXaNRZ0LEP1Dhc6uh19Pm_PYP7l8tKg5Z_dGgnFWwJp2SDweU7kvWgEUEPJVa-
HKd7iiRGP-
2cttS8ak4z1q_OjKkFRHi6A2uZ95Yg0dkWgBbHgCHbbuM5oBmIztFixmnHeoTrV3HPbBPw2jEX_
XINhFVcYnfc1efs0Gh-
jKA4wrCgStq5bXRhMC5degaoQ0Sb5eY_S_Ehpz1yoA_JYDhp6t8FfnSMTNbM9LfoBTgZDdlrRmw
d2dBVJxzkbhTpXo4dpShFRsL1vs0GV3wdELBuzMb3UaTyu-
rJy_DOb1fPE8pmlC1NS2_WHrVXB0gJf91MaaIup_Fx7tJzSbqiNG9mFj6SQvMk0HvAyI195NpyF
NX33x5NLFnF6125mZdn6MY6nLPeNu9PlyEadZ8uXnMtWfrAOuN83yS2XZDWKHPYSJOaVcsGAjRr
cGLpulp-dcx1g0XVQgNR0KzaH7J3zbRJ-Lqf7V6w9aYT1JnHk2lbof2oGp9NaWN1-
Tql0EvrAk3-
EqzyCigOG5A2YZdoRR_1rlCxfNCXz0dtRwM07IX_kEEEEKHTs41k970YTSa_SdhYNMUN0QPBLkjT
ts_YMnx8Y2wFumFy9Ji3K5o2GHB5nc0a1DioSi9gNEpfjv6pT_Tk9NDIFUBAwv8oV_qp41qFqSp
A9g6G51madn0K6sonvAsRlDWNjxSBropglstgWWCre3Ucp_b9PhZhtlrSuJsZynEqLCf9ZLn21x
fugLbIOdvaNZxkI2NtNHCv_CsiMfo76rc5SwCJ5uTtD64z53s2txbOPmhWpIGE63OKi3fQSZz5H
ZdBbidIRcm3vCEseMNw1A27F7_BCIN6o9tZd-lX0Zkvh08Wts2d-clFs-
x5ssLWeoMPPGvnFjZ9pQBD8EyK34JsA5qPTVjLOD62ZRph8PdkiJIoEOes4QMyLeVbUe9rbScIN
F2m5YSHiRWWM5MFSpDFmT67EtriseeWQnVNQTU31_chDRut92yv2G3seSa8HHMLW0Gmq7W7hUUG
uxLbUSVv74U7_55vpQM0fuRhJ7khTbZioN-
wBp32Zyy_phgMi5sOqV35lPoCzpZ7ueQwbsS6kvABCj2PjoeQL2trqrjcfkPflPUKsETgkVrgvi
jt55bzKmUG624fv1zJbgSt7t3rrPiVQyKfLW0YJcx-
39sKDICQeEFpQp_7gnf7LoKKVPAISDLSSCHJro6R5Vm74INsQQjGn-
fH55R2sS4GVw74DfWF1k7wp9Upw3JjlgQ9MhRpVjUd98CprL-
jjdn4k4CuHxZPXEOXEfkvC8PO4HmDN1Od-
3ShVrilhJ1gLFpuM1814OylUju9bhHEM8R28YL7ftgWvtzhMkdw3BPM05Uzo29xAsS_GZeDikFl
db2E7CoZu3evhnrMsk9KWGbbrrxcAZDFR1zhNJHJBVFVpjpjpxgoXy6Br3LAtZBnu217Zt5mfAF08h
EG0baz-MS0hPahcfoE3S7c5xPcV4wTmmX_r9pE_eg-
6tyiylj5I9hOpGUMtogAgRSNA8VP5YLvoDv5D3eMhK_ZzTQtQGEQulpA86uPKjImusrAe4XAbFE
fWIPZ--S6xkYacgCzGjQfAQOInmRLg_fOcmuy2atMbCX9Rf66rbGhOTwIY-HEBUAeIA9cY_AL-
rb78ErzcKhRodnAN3XXq-rpA9709UjBiFm_SEPGESa6HlmxDoPFubEt1g-

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

36CxG41OLaKSEAXPum105xNWUHS_xOaT55mq4DgaX_3cn8q6za9729x3PiGwtw0LhlhH-sezEb7wkSW0HjJoXkRKAMKD_HcaV7cAcwiMEvvE3sX_JQ.m0uVEEEqSLHJRbG-xLOsyA

تکه کد زیر به زبان جاوا با در اختیار داشتن فایل کلید خصوصی امضا و گواهی امضای مودی و همچنین کلید عمومی سرور و شناسه‌ی آن کلید، از روی صورت‌حساب داده شده، بسته‌ی امضا شده و رمز شده 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();

```

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

```

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

jwe.setAlgorithmHeaderValue(KeyManagementAlgorithmIdentifiers.RSA_OAEP_256);
;
jwe.setEncryptionMethodHeaderParameter(ContentEncryptionAlgorithmIdentifiers.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 پیاده سازی شده اند و تنها با فراخوانی یک تابع می توان از آن استفاده نمود. تکه کد ارائه شده صرفاً به منظور آشنایی دقیق تر با فرآیند تولید بسته ای امضا شده و رمز شده ی صورت حساب می باشد. در این بخش هم برای عملیات تولید JWS و JWE از کتابخانه jose-4j نسخه ی ۰.۹.۳ استفاده شده است. همچنین تکه کد زیر به زبان NET. همین عملیات را پیاده سازی می کند:

```


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());
    }
}

```


شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

```

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 رمزنگاری 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:

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

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

با استفاده از این API شرکت معتمد می تواند تمامی صورتحساب های مودیان مختلفی که دسترسی ارسال صورتحساب را به شرکت معتمد واگذار کرده اند ارسال نماید و نیازی نیست تمامی صورتحساب های موجود در یک درخواست متعلق به یک شناسه یکتای حافظه مالیاتی باشد. همچنین مودی می تواند در یک درخواست ارسال صورتحساب، صورتحساب های مربوط به شناسه یکتاهای مختلف خود را ارسال نماید. البته شناسه یکتاهایی که اجازه ی ارسال صورتحساب از طریق آن ها 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 خطا مواجه می شود. همچنین در صورتی که ارسال کننده درخواست برای یک شناسه

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		


```
{
  "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 می شوند.

۸-۱- استعلام صورتحساب به وسیله شماره پیگیری

به وسیله ای این API می توان وضعیت صورتحساب ارسالی را با استفاده از کد پیگیری ای که وب سرویس جمع آوری به ازای هر صورتحساب در اختیار قرار می دهد استعلام نمائیم. نحوه ی کار این API به صورت زیر است:

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

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

<p>آرایه‌ی JSON شامل اشیائی با محتویات زیر (به ازای هر شماره پیگیری یک شیء JSON در این آرایه برگردانده می‌شود):</p> <ul style="list-style-type: none"> • referenceNumber: شماره پیگیری درخواست اعلام شده • uid: شناسه درخواست (همان requestTraceId که صورتحساب با آن ارسال شده بود) • status: وضعیت صورتحساب دارای حالت‌های زیر: <ul style="list-style-type: none"> ○ 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 صف بررسی می‌باشد. ○ NOT_FOUND: شماره پیگیری داده شده یافت نشد. • data: لیست خطاها / اخطارهای موجود در صورتحساب • packetType: نوع بسته • fiscalId: شناسه حافظه ارسال‌کننده‌ی صورتحساب • sign: امضای پاسخ به فرمت بسته‌ی JWS که ساختار آن در جدول بعدی توضیح داده می‌شود (فقط در حالت SUCCESS) 	خروجی
--	-------


همانطور که گفته شد خروجی درخواست اعلام 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:

امضای پاسخ نتیجه‌ی اعتبارسنجی صورتحساب – JWS	
<p>یک شیء JSON دارای فیلدهای زیر:</p> <ul style="list-style-type: none"> • alg: الگوریتم امضا: RS256 • sigT: زمان امضای توکن <p>Format: yyyy-MM-dd'T'HH:mm:ss'Z' Example: 2023-05-13T10:44:47Z</p>	Header
<p>شیء JSON دارای فیلدهای زیر:</p> <ul style="list-style-type: none"> • referenceNumber: شماره پیگیری درخواست صورتحساب ارسالی. مثال: 	Payload


```
"uid": "2b982bfd-9a60-47cd-9da7-30fc0dabd37d",
"status": "FAILED",
"data": {
  "error": [
    {
      "code": "012802",
      "message": "مجاز مقادیر جز «تسویه روش» فیلد در شده وارد مقدار",
      "errorType": "ERROR"
    }
  ],
  "warning": [],
  "success": false
},
"packetType": "receive_invoice_confirm",
"fiscalId": "A111OK",
"sign": ""
},
{
  "referenceNumber": "f9173085-2316-4ca6-918e-e41aaef7ef8dd",
  "uid": "c5352f85-9322-41bc-a5b2-9abb130fe622",
  "status": "SUCCESS",
  "data": {
    "error": [],
    "warning": [],
    "success": true
  },
  "packetType": "receive_invoice_confirm",
  "fiscalId": "A111OK",
  "sign":
"eyJhbGciOiJSUzI1NiIsInRheElkiOiJMTNUMTE6NTI6NDIuOTgyWiJ9.lanl052gttnAp6F1MX9NxPn9swN4-IjFiowTX2ytm_1YgAqgzBLytvTBRrq_NoPeIH9LIRd275iFJaysMxbFmVnstTLp91hg_iMGAXxwY5EL_LYnexu-
biPSswfTXK9lf6RjKrIIDm0hyBr2pCZpc_ZXSgwLHyaf1p_GgxvYSql4l3xCNzzFKfp3yI8
hiHovmUlkbdrIH_YXKckDw9ZlH6a3NcVsImj65Ed7pemBMmJLPf_Kj7tn7e8s4dUGh0fs6H
fCB7LMDejPDu6jgbIPkwANHWaxx3dZOeO3bUKSo6SIyInvo3GQvDP5dpYGngkQ9NAme7HKg
HjDHJJzEcjkACG-
Gj3LEsyQveHrL4s5q9YGYWwavZVinbTRMwl75_LRgIeB1UuWNVLS5PtSk2o6drzRnNJ6iN5
tOvnF_y8J57oO1LHXDtPMs5ncQF2e_NJ2tGmFxQs868T1ODggaHzBc3H7VyQ8KC1uD_W3ZA
1ErKbAdvT2eDHZVFHoREZVoYW3m7graO5fiYcYUle9TUXLARQwd_ihEcKbRtLbtw42ZHqfX
Q77vJdY79XB8OkUjA5kfJ6g4o80Qqa-NaIoeWrFte0g5e-
SUSJklnd4pZTTApZfCMongoKFSGJ0USfi0T3M-OX7lyxJbOYKeqUzt4"
}
]
```

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

۸-۲-۸ استعمال با uid

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

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

Inquiry by uid – استعلام به وسیله شناسه درخواست	
https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-uid	آدرس
GET	Method
<p>فیلدهای زیر:</p> <ul style="list-style-type: none"> uidList: لیست شناسه درخواست‌های صورتحساب‌های مورد نظر fiscalId: شناسه حافظه صادر کننده صورتحساب start: شروع بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T00:00:00.000000000+03:30 end: پایان بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T23:59:59.123456789+03:30 <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.</p> <p>محل قرارگیری: Request Params</p>	ورودی
دقیقاً 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=A111Y0&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": [
        {

```


شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

۸-۳- اعلام براساس بازه زمانی


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

Inquiry - اعلام در بازه زمانی	
https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry	آدرس
GET	Method
<p>فیلدهای زیر:</p> <ul style="list-style-type: none"> pageNumber: شماره صفحه (مقدار پیشفرض: ۱) pageSize: اندازه‌ی صفحه (مقدار پیشفرض: ۱۰ - مقادیر مجاز: ۱ تا ۱۰۰) status: وضعیت صورتحساب‌هایی که به دنبال آن هستیم. <ul style="list-style-type: none"> مقادیر مجاز: SUCCESS, FAILED, TIMEOUT, IN_PROGRESS در صورتی که این فیلد خالی باشد همه‌ی صورتحساب‌ها برگردانده می‌شود. start: شروع بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T00:00:00.000000000+03:30 end: پایان بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T23:59:59.123456789+03:30 <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.</p> <p>محل قرارگیری: Request Params</p>	ورودی
دقیقا همانند اعلام با شماره پیگیری و uid	خروجی

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:

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

```
6fk4IhQU08KkpD37HMTCTNHur33dFQ_qDHG4zcttGI1Q41j7f6FwP8c1wW59oVCAJfLyekJjGr5
a0aqJtQXF3G5YwBzfQmtRj6hP62cyWC5ixv8"
}
]
```

۹ – 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 برمی گرداند. نحوه ی کار این API به صورت زیر است:


GET Fiscal Information – دریافت اطلاعات حافظه	
آدرس	https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information
Method	GET
ورودی	<ul style="list-style-type: none"> memoryId: شناسه حافظه مورد نظر محل قرار گیری: Request Params
خروجی	<p>شیء JSON شامل فیلدهای زیر:</p> <ul style="list-style-type: none"> nameTrade: شناسه حافظه fiscalStatus: وضعیت حافظه nationalId: شناسه ی ملی پرونده / کد ملی صاحب پرونده economicCode: کد اقتصادی پرونده

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"
}
```

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

۹-۲- اطلاعات مودی

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


GET Taxpayer - دریافت اطلاعات مودی	
https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer	آدرس
GET	Method
<ul style="list-style-type: none"> economicCode: شماره اقتصادی مودی 	ورودی
<ul style="list-style-type: none"> محل قرار گیری: Request Params 	
<ul style="list-style-type: none"> شیء JSON شامل فیلدهای زیر: nameTrade: نام مودی / پرونده اقتصادی taxpayerStatus: وضعیت پرونده شامل فیلدهای: «NOT_ALLOCATED» به معنی تخصیص نیافته، «ACTIVE» به معنی فعال مجاز، «DEACTIVATED» به معنی غیر فعال (عبور از حد مجاز ماده ۶)، «TEMPORARY_UNAUTHORIZE» به معنی غیر مجاز موقت، «PERMANENT_UNAUTHORIZE» به معنی غیر مجاز دائم و «ARTICLE_2_SUBJECT» به معنی مشمول تبصره ماده ۲ می باشد. 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=14003778990' \
-H 'accept: */*' \
-H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXZXQOM-_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"
}
```


شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

۱۰- استعلام وضعیت صورتحساب در کارپوشه

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

GET Taxpayer - دریافت اطلاعات مودی	
آدرس	https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-invoice-status
Method	GET
ورودی	<ul style="list-style-type: none"> taxIds: لیست شماره مالیاتی صورتحساب محل قرارگیری: Request Params
خروجی	<p>شیء JSON شامل فیلدهای زیر:</p> <ul style="list-style-type: none"> taxId: شماره مالیاتی ارسالی invoiceStatus: وضعیت صورتحساب دارای مقادیر زیر: <ul style="list-style-type: none"> REJECTED (رد شده) APPROVED (تایید شده) SYSTEMIC_APPROVED (تایید سیستمی) IMPOSSIBLE_REACTION (عدم امکان واکنش) AWAITING_REACTION (در انتظار واکنش) NO_NEED_REACTION (عدم نیاز به واکنش) CANCELED (باطل شده) DELETED (حذف شده) SYSTEMIC_REJECTED (رد سیستمی) article6Status: وضعیت عبور از حد مجاز ماده ۶ دارای مقادیر زیر: <ul style="list-style-type: none"> EXCEEDED (عدول) NOT_EXCEEDED (عدم عدول) error: خطا، دارای مقادیر زیر <ul style="list-style-type: none"> NOT_FOUND (صورتحساب یافت نشد) ACCESS_DENIED (دسترسی ندارید)

نمونه درخواست ارسالی:

شناسه سند	<p>سند «دستور العمل فنی اتصال به سامانه مودیان»</p>	 <p>سازمان امور مالیاتی کشور</p>
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

```
curl -X 'GET' \
  'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-invoice-
status?taxIds=A111DW04E8300004349008&taxIds=A111DW04E8300003CC4EA5' \
  -H 'accept: */*' \
  -H 'Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXOM- 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 - ییوستها

۱۱-۱- گواهی و کلید خصوصی امضا

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

```
-----BEGIN CERTIFICATE-----
MIIDejCCAmKgAwIBAgIUUV27QXqJjK2EgFy9zeYkpsX+ISPswDQYJKoZIhvcNAQEL
BQAwcTELMAkGA1UEBhMCsvIXDDAKBgNVBAGMA1RlaDEMMaAoGA1UEBwwDVGVomREw
DwYDVQQKDAhNb2hhew1lbjEMMAoGA1UECwwDVGVf4MSUwIwYJKoZIhvcNAQkBFhZt
Lm1hbHZ1cmRpQG1vaGF5bWVuLmlyMB4XDTIzMMDMyNDEzMjgyM1oXDTI0MMDMyMzEz
MjgyM1owTTEPMA0GA1UEAwwGQW56YXpMRcwFQYDVQQKDA5RdW9WYWRRpcyBHcm91
cDELMakGA1UEBhMCsvIXFDASBgNVBAUTCzE0MDAzNzc4OTkwMIIIBiJANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEazLgyk5KO6+j9d1ud0ilJArrZ3Whw/w9wEzHB
9yXwENRa5fm5AbRukMF5b6VGeKzD6LZuL9+tfdfFwyPcjI++gGNyWzRmEHKpTnzP
1t6NyuXKfm4nBVAb1sugSw8Y5DEXRftqILgBWN/pZ4zGlfEALMcGAs7ADcjnv7b
/tM2wxr9rHxsCvW4Hv1zQask8Qr1CrKgT0EI66rSXCHep/uIONDwp0W20e1M1ZtM
6AAjWXRlGcshPIHuK+ZLfAFxWtoGonf6qN9ypos2B18D/EFa8WHON62eYKT0kW3j
```

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 سازمان امور مالیاتی کشور
RC_TICS.IS_v1.4		
بهمن ۱۴۰۳		

BVa3yPEkRwkdDjDu/3CPzymhf3WFYwxb4t35oWb/qUXGVI dvwIDAQABoy4wLDAfBgNVHSMEGDAWgBSx+Oq+R03x/FmyCp+jcmfOH+Fn9TAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQAqKATXlnS+pPtAiRIYGtydVU5Vi7Aq+D6QW07uFqcB7vBhddN3yX21LVcwptNjzhv8UCM+mDMvlmsRVKvtMoo5fHfII92/Wo8rUz1RP+yhyCk0Vz8I11v+bjLwVur/agC/s5Rf0m66pNNjFZ9J3S2N31ChXYwz2vvA8pdAYvWTu9g5u4FMFqlsaLwMGC+WaA0g3KYzRkdWRy1vd23hLTUcVsWM8wpgZ11wEGE1khca/Sd0mCU2HG5vIbqFfTjA6to0fY07CE5fD8aR3UcXjNduosV052ZqCX5SabrhFS3AGHFRjpFnI5LZespiCXSA8Sv3k0SCSRQKqFbiwSFM8Zjg

-----END CERTIFICATE-----

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

-----BEGIN PRIVATE KEY-----

MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBAwggSjAgEAAoIBAQMduDKTko7r6P13W53SKUkCutndaHD/D3ATMcH3JfAQ1Fr1+bkBTG6QwXlvpUZ4rMPotm4v36190V9bI9ymJ76AY3LDNGYQcql0fM/W3o3K5cp+bicFUBuWy6BLDxjkmRdF90oguAFY3+lnjMaWJ8QAsxwYCzsAny0e/tv+0zbDGv2sfGwK9bge+XNBqwrxCvUKsqBPQQjrqtJcId6n+4g40NanRbY56UyVm0zoACNZdEsZyyE8ge4r5kt8AXFa2gaid/qo33KmizYHXwP8QVrxYc43rZ5gpPSRbeMFVrfI8SRHCR0M07/cI/PKaF/dYVjdGLvi3fmhZv+pRcZUh2/AgMBAAECggEACPPc7YnNzram9ucDosXAt+ftyfHckrLgnVbfRLfBN8G4QsGSxWpeNub1Jmo/Due0p63oYx0SBKR75AlmKLV1CzhRPhI8L5h3qEN88dVMrospOCYoe+kpbJF9dA0zcD5e40h+o/StynH3UF0yED+qLsWsA7nqWnYQj9ZpW2Fz01Z1i5NRX4YgyIopHfqcLWJWpOR8n4HwDY18BL7tMi31f0sZXz56EUgBPxq5RMi+1iKWpyZdwy4TrJL/Sj4tWkKJ7ELVd47VunizAqeLDy8bL1PBX0PewRvR37P9axHLjsj/d1Iw/xvqgVEWZTyUXzg4qgFU5Na5u6xIW8JyqejdEQKBgQD2Q1DdoP0tG1URyuu04HJ1Q85ZFEWAA0vvp8esvJLJ7t73Rz28RkKAMHW/njr23ExxV3eek9J11GENJUZFKsNNTjRWMgCxCuic00MGTJuraWHrEma00YNNjpVd3pIi68p51CZNzMRLn2J8F+7CPeGiynKEvKU43KcJr6K0kWP14FQKBgQDU0T3SNr7af4y3r03ds2DMaoKEG531tuLunrZNnL4a/i2r3AlI5K470UkmAXDD1kgGf235KxrRm7x7VVp5SZLgOPqgJ20KKk9bHLvuAdxCeUlnDfJWrAmYcmYLLCSDHBudN/evF6WiNaQi074MhdbaxYdLiiXdS3VVf1Q/8m6/gwKBgD4ijXTeX52V/+j1YnDB8RtL+IzrpkMrocVeeCtFiwQa0Xf7KcCPmcfuckdfDVGSVD1k7HG+qqOwRKykCw6Qs6awCpSVGUekiuZaFf2jHC7r1E522BUXOT8zQNaXVUiWXXt4zZOLFlIZfkZsMyiAISqwCptzuKCCKOPZVzDoo0vhAoGBAMo82XnVyoKLKwC2r4i600eo48S1FeP12yuVqXqR1FqEZ1RlMnGR1z1DAjdasRV5oVKDcDeTzdWZIIIE3uFWAJFJt80WUinQ4ptbXtINWQ0DsT2PebggNTsUPH7UVytDJ0jiqgfZjC2TdgTAR1g3Cdk3J3mtbqeXlGmiXN2rZcIMPAoGADfTonaehrsnscUch4DgsqZdyZm9JRmoNyisLBmbGkTNxoY09Vm/03u3NMsohkjopt2ly38ZMYX14FyXKEKcI977r33JD9PxRcovqFhcPR3WuQrPf6ND3IX6eB5p8d7m6fmFYSe/0NhWoeH99a6/csAr2hPMOb/R3GdRwksGgQ=

-----END PRIVATE KEY-----