



---

# مرکز تنظیم مقررات نظام پایانه‌های فروشگاهی و سامانه مودیان

---



سند

«دستورالعمل فنی اتصال به سامانه مودیان»

شناسه سند:

RC\_TICS.IS\_v1.3

مهر ۱۴۰۲



شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

## 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 چهارچوب REST API پیاده سازی شده و فراخوانی آن نیازمند احراز هویت<sup>۱</sup> مودی از طریق امضای دیجیتال می‌باشد.



در این سند منابع موجود در این وب‌سرویس 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.

<sup>۱</sup> Authentication

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

## فهرست مطالب

تعاریف.....	۴
دریافت شناسه یکتای حافظه مالیاتی.....	۵
مراحل ارسال صورتحساب و استعلام وضعیت آن.....	۶
منابع در دسترس و کاربردهای هر کدام.....	۶
دریافت چالش تصادفی و احراز هویت.....	۹
دریافت اطلاعات سرور.....	۱۷
ارسال صورتحساب.....	۱۸
استعلام وضعیت صورتحساب‌های ارسالی.....	۳۳
استعلام اطلاعات حافظه و مودی.....	۳۹
پیوست‌ها.....	۴۲



شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

## ۱ - تعاریف

عنوان	تعریف
امضای دیجیتال <sup>۲</sup>	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 <sup>۳</sup>	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 <sup>۲</sup>

Digital Signature Certificate <sup>۳</sup>

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

## 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:

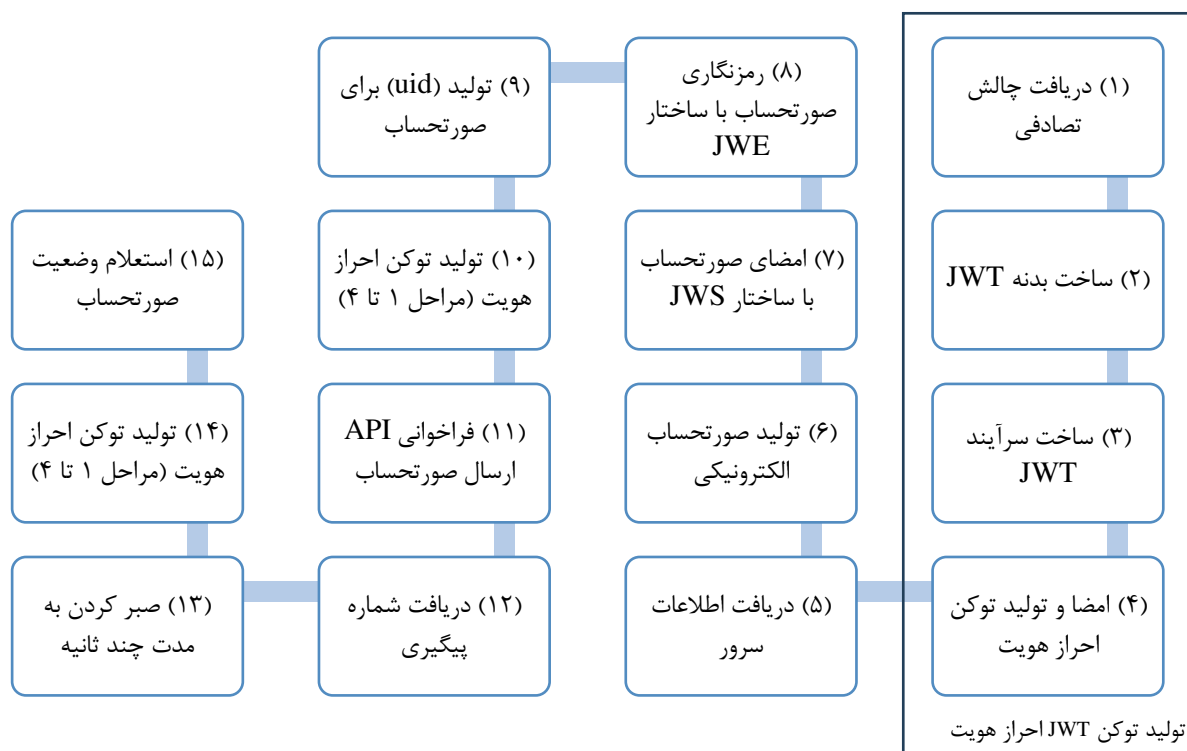
۱. به ازای هر شناسه یکتا حافظه مالیاتی، یکی از سه حالت ارسال اطلاعات صورتحساب را به شرح ذیل انتخاب کند:

- 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 (v1.2) 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 <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/nonce">https://tp.tax.gov.ir/requestsmanager/api/v2/nonce</a>	<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 <a href="#">راهنما در صفحه ۱۰</a>
POST <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/invoice">https://tp.tax.gov.ir/requestsmanager/api/v2/invoice</a>	<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 <a href="#">راهنما در صفحه ۱۸</a>
GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer">https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer</a>	<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>	<pre>{   "nameTrade": "string",   "taxpayerStatus": "string",   "taxpayerType": "string",   "postalcodeTaxpayer": "string",   "addressTaxpayer": "string" }</pre>	دریافت اطلاعات پرونده‌ی مودی <a href="#">راهنما در صفحه ۴۰</a>
GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information">https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information</a>	<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",   "saleThreshold": "string",   "economicCode": "string" }</pre>	دریافت اطلاعات حافظه <a href="#">راهنما در صفحه ۳۹</a>
GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/server-information">https://tp.tax.gov.ir/requestsmanager/api/v2/server-information</a>	<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 <a href="#">راهنما در صفحه ۱۷</a>

استعلام صورتحساب با شماره پیگیری <a href="#">راهنما در صفحه ۳۳</a>	<pre>[ {   "referenceNumber": "string",   "uid": "string",   "status": "string",   "data": {},   "packetType": "string",   "fiscalId": "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%3A00.000000000%2B03%3A30&amp;end=2023-05-14T21%3A00%3A00.000000000%2B03%3A30' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGc...[JWT TOKEN]...q4RcXogA'</pre>	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>
استعلام با شناسه درخواست (uid) <a href="#">راهنما در صفحه ۳۵</a>	<pre>[ {   "referenceNumber": "string",   "uid": "string",   "status": "string",   "data": {},   "packetType": "string",   "fiscalId": "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%3A00.000000000%2B03%3A30&amp;end=2023-06-10T23%3A59%3A59.999999999%2B03%3A30' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGciO...[JWT TOKEN]...ski8e-A'</pre>	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>
استعلام براساس بازه زمانی <a href="#">راهنما در صفحه ۳۷</a>	<pre>[ {   "referenceNumber": "string",   "uid": "string",   "status": "string",   "data": {},   "packetType": "string",   "fiscalId": "string" } ]</pre>	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry?start=2023-06-10T00%3A00%3A00.000000000%2B03%3A30&amp;end=2023-06-10T23%3A59%3A59.999999999%2B03%3A30&amp;pageNumber=1&amp;pageSize=10' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGciO...[JWT TOKEN]...KXzBjRZw'</pre>	GET <a href="https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry">https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry</a>

جدول ۱



شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

## 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<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. 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.

<sup>۴</sup> Nonce

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

## 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"> <li>timeToLive: مدت زمان اعتبار رشته تصادفی به ثانیه <ul style="list-style-type: none"> <li>نوع ورودی: اختیاری</li> <li>محل قرارگیری: Request Params</li> <li>مقدار پیش فرض: ۳۰</li> <li>مقادیر مجاز: ۱۰ تا ۲۰۰</li> </ul> </li> </ul>
خروجی	<ul style="list-style-type: none"> <li>nonce: رشته تصادفی تولید شده</li> <li>expDate: زمان انقضای رشته تصادفی</li> </ul>

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»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

ساختار توکن JWS	
<p>یک شیء JSON دارای فیلدهای زیر:</p> <ul style="list-style-type: none"> <li>alg: الگوریتم امضا: 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>○ فرمت:</p> <pre>yyyy-MM-dd'T'HH:mm:ss'Z'</pre> <p>○ نمونه:</p> <pre>2023-05-13T10:44:47Z</pre> <ul style="list-style-type: none"> <li>typ: رشته "jose"</li> <li>crit: لیستی از فیلدهای ضروری در قسمت Header. تنها شامل رشتهی "sigT"</li> <li>cty: رشتهی "text/plain"</li> </ul> <p>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> <pre>2023-05-13T14:14:47Z+0330</pre> <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>	Header
<p>یک شیء Json دارای دو فیلد زیر:</p> <ul style="list-style-type: none"> <li>nonce: رشته تصادفی یکبارمصرف دریافت شده</li> <li>clientId: شناسه ارسال کننده صورتحساب</li> </ul> <p>○ برای مودیان همان شناسه حافظه صادر کننده صورتحساب</p> <p>○ برای شرکت‌های معتمد شناسه شرکت معتمد</p>	Payload



شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

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

```
{ "nonce": "942a1ccd-a6a5-47f6-8e80-a92358cc11a1", "clientId": "A11226" }
```

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

توکن JWT ساخته می‌شود:

```
eyJhbGciOiJSUzI1NiIsIng1YyI6WyJNSU1EZWpDQ0FtS2dBd0lCQWdJVVYyN1FYcUpqSzJFZ0Z5OXplWWtwc1grSVNQc3dEUUVlKS29aSWh2Y05BUUVMQlFDb2NURUxNQWtHQTFVRUJoTUNTUk14REBS0JnTlZCQWdNQTFsbgFERU1NQW9HQTFVRUJ3d0RWR1ZvTVJFd0R3WURWUVFLREFOcTmIyaGhlVzFsYmpFTU1Bb0dBWVVFQ3d3RfZHRjRNU1V3SXdkZSkvtWklodmNOQVFrQkZ0WnRmBTfoYkhabGntUnBRRzF2YUdGNWJXVnVMBWx5TUI0WERUSXpNRE15TkRFeK1qZ3lNMW9YRFRJME1ETXlNekV6TWpneU0xb3dUVEVQTUEwR0ExVUVBd3dHUvc1N1lXeHBNUmN3RlFZRFZRUUteEQTVSZFc5V1lXUnBjeUJlY205MWNERUxNQWtHQTFVRUJoTUNTUk14RkRBU0JnTlZCQVUQ3pFME1EQXpOemM0T1Rrd01JSUJJaFQ0mdrcWhraUc5dzBCQVFFRkFBT0NBUThtBTU1JQkNnS0NBUEVBekxneWslS082K2o5ZDF1ZDBpbEpBcnJAMldody93OXdfekXCOX1Yd0VOUmElZm01QWJSdWtNRjViNlZHZUut6RDZMWNVMOST0ZmRGZld5UGNqSSsrZ0dOeXd6Um1FSEtwVG56UDF0Nk55dVhLZm00bkJWQWJsc3VnU3c4WTVERVhSZlRxsUXnQldOL3BaNHpHbGlmRUFTMTWNHQM3QURjam52N2IvdE0yd3hyOXJlIeHNDdlc0SHZse1Fhc0s4UXIxQ3JLZl1QWRUk2NnJTWENIZXAvdU1PTkRxcDBXMk9lbElswNnRNNkFBaldYUkxHY3NoUElIdUsrWkxmQUZ4V3RvR29uZjZxTj15cG9zMkIxOEQvRUZhOFdIT042MmVZS1QwalczakJWYTN5UEVrUndrZERqRHUvM0NQenltaGYzv0Zzd3hwYjR0MzVvV2IvcVVRl1ZJZH3SURBUUFCb3k0d0xQWZCZ05WSFNNRUdEQVdnQlN4K09xK1JPM3gvRm15Q3AramNtZk9IK0ZuOVRBSkNjTlZlUk1FQWpBQU1BMEdDU3FHU01lM0RRRUJdDlVBQTRJQkFRQWdLQVRYbG5TK3BQdEFpUk1ZR3R5ZfZVNVZpN0FwK0Q2UUVcwN3VGcWNCN3ZCaGRkTjN5WDJsVlZjd3BUTkp6aHY4VUNNK21ETXZsbXNSVktWdElvbzVmSGZJSTkyL1dvOHJVeJFSUCt5aHlDazBWejhJMTF2K2JqTHdWdXlVYwDdL3M1UmYwbTY2cE5OakZaOUozUzJOM2xDaFhZd3oydnZBOHBkQVl2V1RlOWclDRGTUzxbHhNThdNR0MrV2FBMGczS1l6Umtkv1J5MXZkMjNoTFRVY1ZzV004d3BnWjExd0VHRTFragNhL1NkMG1DVTJIRzV2SWJxRmZUake2dG8wZlkwN0NFNWZEOGFSM1VjWGpOZHvc1ZPNTJacUNYNVNHYNJoRlMzQUdIRlJqcEZuSTVMWmVzcGlDWfNBOfN2M2tPU0NTU1FLcUZiaXdTRk04WmpnIl0sInNpZlQiOiIyMDIzLTA1LTEzVD EwOjQ0OjQ3WiIsInR5cCI6Impvc2UiLCJjcml0IjpbInNpZlQiXSwiY3R5IjoiaGV4dC9wbGFpb iJ9.eyJub25jZSI6IjK0MmExY2NkLWE2YTUtNDdmNi04ZTgwLWE5MjMlOGNjMTFhMSIsImNsaWVudElkIjoiaQTEuIn0.fliLj8jt6Z-vZCS1A6Rm2KaEEGIVko6gPyNO5qjd6I0cSDVPFsrElBXhvTprn3lBRipro8-XUNDzgPtqOB9CYyC2kscULBKsUybTJJKEm8FfvfLXsRTdTYqvcOFjdgxnwSdGVi3KwL-2wFjG10xe_vcIYOR7-xd4o5ON5t7CGChe7u01ZY-luxabzx8svvjXpA2QGBbMTwBXwToLcnpr27VGySzIr8bROYgKh1l2v4RU-XzX4w3a09fm-scrhs2TTJ1h7V1G_ALArhtbZeJ1Umz-XBM0ZxHj11m8_gyVPLM70yB7SN5uqfRShdJiK05TWLsN7NeIPV670dAVD5imfA
```



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

این فرایندها در کیت توسعه نرم‌افزاری 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();
```

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

```

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\":\"942a1ccd-a6a5-47f6-8e80-
a92358cc11a1\",\"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("typ", "jose");
jws.setHeader("crit", new String[]{"sigT"});
jws.setContentTypeHeaderValue("text/plain");

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-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;

```

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

```

using JWT.Algorithms;
using JWT.Builder;
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\":\"942a1ccd-a6a5-47f6-8e80-
a92358cc11a1\",\"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("typ", "jose")
            .AddHeader("crit", new[] {"sigT"})
            .AddHeader("cty", "text/plain")
            .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" />

```

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

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

حال باید با استفاده از این توکن هنگام ارائه درخواست بعدی خود را به سرور معرفی نمائیم. بدین منظور باید در سرآیند<sup>۶</sup> 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.

<sup>۶</sup> Header



شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

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	<p>شیء Json دارای فیلدهای زیر:</p> <ul style="list-style-type: none"> <li>serverTime: برچسب زمانی سرور</li> <li>publicKeys: آرایه Json از کلیدهای عمومی رمزگذاری سرور هر یک شامل:</li> </ul>

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

○ 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+Wm1lhzzjhAGfSUOuDVOKRoUEQwP8oUcXRmYzcvCUgcFoRT5iz7HbovqH+bIeJwT4rmLm
      FcbfPke+E3DLUxOtIZifEXrKXWgSVPkRnhMgym6UiAtnzwA1rmKstJoWpk9Nv34CYgTk8DKQN5j
      QJqb9L/Ng0zOEEtI3zA424tsd9zv/kP4/SaSnbbnj0evqsZ29X6aBypvnTnWH9t3gbWM4I9eAVQ
      hPYClawHTqvdaZ/O/feqfm06QBFnCGl+CBdjLs30xQSLsPICjnlV1jMzoTznAabWP6FRzzj6C2s
      xw9a/Ww1XrKn3gldZ7Ctv6Jso72cEeCeUI1tzhMDJPU3Qy12RQzaXuJpMhCz1Dva47RvqiumpTN
      yK9HfFIdhgoupFkxT14XLD16S55MF6HuQvo/RHSbBJ93FQ+2/x/Q2MNGB3BXOjNwM2pj3oJbDv
      3pj9CHzvaYQUYM1yOcFmIJqJ72uvVf9Jx9iTObaNNF6p152ADmh85GTAH1hz+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 همه‌ی 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»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

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

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

<ul style="list-style-type: none"> <li>• typ: رشته "jose"</li> <li>• crit: لیستی از فیلدهای ضروری در قسمت Header. تنها شامل رشته‌ی "sigT"</li> <li>• cty: رشته‌ی "text/plain"</li> </ul>	
شیء JSON صورتحساب	<b>Payload</b>
ورودی الگوریتم امضا: ASCII (BASE64URL (UTF8 (JWS Protected Header))    '.'    BASE64URL (JWS Payload)) الگوریتم: RSASSA-PKCS1-v1_5 using SHA-256 کلید خصوصی: کلید خصوصی متناظر با گواهی فرستاده شده در بخش Header	<b>Signature</b>

ساختار بسته‌ی JWS صورتحساب دقیقاً مانند توکن JWS می‌باشد. با این تفاوت که payload آن JSON صورتحساب می‌باشد. توجه کنید که رشته‌های Header و Payload باید به فرمت utf8 بوده و برای 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, "tvam": 1755, "todam": 0, "tbill": 21255, "setm": 2 }, "body": [ { "sstid": "2710000138624", "sstt": "فولاد صنعت قطعات سرسیلندر", "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 Header آن مقدار زیر باشد:

```
{ "alg": "RS256", "x5c": [ "MIIDEjCCAmKgAwIBAgIUUV27QXqJjK2EgFy9zeYkpsX+ISPswDQYJKoZIhvcNAQELBQAwTElMAkGA1UEBhMCsvIxDDAKBgNVBAGMA1RlaDEMMMAoGA1UEBwwDVGVomREwDwYDVQQKDAhNb2hheW1lbjEMMAoGA1UECwwDVGV4MSUwIwYJKoZIhvcNAQkBFhZtLm1hbHJlcmRpdG1vaGF5bWVuLmlyMB4XDTEzMMDMyNDZmZjYmIwXDTI0MDMyMzEzZjYmIwYDTEPMA0GA1UEAwGQW56YXpMRcwFQYDVQKDA5RdW9WYWRpcyBHcm91cDELMAMGA1UEBhMCsvIXFDASBgNVBAUTCzE0MDAzNzc4OTkwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEazLgyk5K06+j9dlud0ilJArrZ3Whw/w9wEzHB9yXwENRa5fm5AbRukMF5b6VGeKzD6LzuL9+tfdfFwYpCjI++gGNyWzRmEHKpTnzPlt6NyuXKfm4nBVAbIsugSw8Y5DEXRfTqILgBWN/pZ4zG1lfeALMcGAs7ADcJnv7b/tM2wxr9rHxsCvW4HvlzQasK8Qr1CrKgT0EI66rSXCHeP/uIONDWP0W2OelM1ZtM6AAjWXRLGcshPIHuK+ZLFAFxWtoGonf6qN9ypos2B18D/EFa8WHON62eYKT0k3jBva3yPEkRwkdDjDu/3CPzymhf3WfYwXpb4t35oWb/qUXGVIdvwIDAQABoy4wLDAfBgNVHSMEGDAWgBSx+Oq+RO3x/FmyCp+jcmfOH+F9TAJBgNVHRMEAjAAMA0GCSqGSIb3DQEBCwUAA4IBAQAqKATXlnS+pPtAiRIYgtydVU5Vi7Aq+D6QW07uFqcB7vBhddN3yX21VVcwPtnJzhv8UCM+mDMvImSRVKvtMoo5fHfII92/Wo8rUz1RP+yhyCk0Vz8I11v+bjLwVur/agC/s5Rf0m66pNNjFZ9J3S2N31ChXYwz2vvA8pdAYvWTu9g5u4FMFqlsaLwMGC+WAa0g3KYzRkdWRy1vd23hLTUcVsWM8wpgZ1lwEGE1khca/Sd0mCU2HG5vIbqFfTjA6to0fY07CE5fD8aR3UcXjNduosVO52ZqCX5SabrhFS3AGHFRjpFnI5LZespiCXSA8Sv3kOSCSRQKqFbiwSFM8Zjg"], "si
```



شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

Ayk8q4iPaTk22x\_TnQQEuRQb3NihZrJULVjDL1VR2fb1R3iZmLGmw\_fcr14wkRrXXqRc-7Ipm8a9FEoeuQZ-ZA9oevg



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<sup>۷</sup> 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 ) 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

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

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

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.

ساختار شیء JWE:

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>	Header سرآیند
<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 می‌کنیم. کلید رمز شده ۵۱۲ بایت طول دارد که Base64URL Encoded آن را در این قسمت قرار می‌دهیم.</p>	Encrypted Symmetric Key کلید متقارن رمز شده
<p>Encode شده‌ی ۱۲ بایت (۹۶ بیت) iv به فرمت Base64URL که رشته‌ای به طول ۱۶ کاراکتر می‌شود.</p>	Initial Vector
<p>رشته‌ی JWS صورتحساب امضا شده که با استفاده از کلید متقارن و با الگوریتم AES256-GCM رمز می‌شود.</p>	Payload محتوای رمز شده
<p>تگی که به منظور اطمینان از دستکاری نشدن محتوای پیام رمز شده و کلیدها استفاده می‌شود.</p>	Authentication Tag تگ شناسایی



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)) || '.' ||



شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

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

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:

```
eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIiwia2lkIjoiaNmEyYmNkODgtYTg3MS00MjQ1LWEeZ0TMtMjg0M2VhZmU2ZTAyIn0
```

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:

```
iLJAHYUaPe6sNSg9GBcV95ZNwFzUxB_w9Nk6gMjA0E
```

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:



```
MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAXdzREOEfk3vBQogDPGTMqdDQ7t0oDhu
KMZkA+Wm1lhzzjhAGfSUOuDVOKRoUEQwP8oUcXRmYzcvCUgcfoRT5iz7HbovqH+bIeJwT4rmLmF
cbfPke+E3DLUxOtIZifEXrKXWgSVPkRnhMgym6UiAtnzWAlrmKstJoWpk9Nv34CYgTk8DKQN5jQ
Jqb9L/Ng0zOEETI3zA424tsd9zv/kP4/SaSnbbnj0evqsZ29X6aBypvnTnwH9t3gbWM4I9eAVQh
PYClawHTqvdaZ/O/feqfm06QBFnCGl+CBdjLs30xQSLsPICjnlV1jMzoTznAabWP6FRzzj6C2sx
w9a/WwlXrKn3gldZ7Ctv6Jso72cEeCeUIltzHMDJPU3Qy12RQzaXujpMhCz1dVa47RvqiumpTNy
K9HfFIhdhgoupFkxT14XLDl65S55MF6HuQvo/RHSbBJ93FQ+2/x/Q2MNGB3BXOjNwM2pj3ojbDv3
pj9ChzvaYQUYm1yOcFmIJqJ72uvVf9Jx9iTObaNNF6p152ADmh85GTAH1hz+4pR/E9IAXUI1/Yi
UneYu0G4tiDY4ZXyKYNknNfhSgxmn/gPHT+7kL3lnyxgjIEEhK0B0vagWvdRCNJSNGWpLtlq4Fl
CWTAnPI5ctiFgq925e+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 RSA-OAEP-۲۵۶ با ورودهای یکسان، متفاوت خواهد بود:

```
XUalzm2Shs7hQut3eHYAgasxvw7_Z4AF6H3fenBXPA_pPz5u9P2v9LkiC-
Qcqy4ADoJcvitpBLuxhvMMp7y8u8tklDV0ALsOYwqsZ2N8ew4oeTy69seeOT0kLeZBcUySkhBs3
FnrkXa0U84XcqWnUypOixKEYH5qG96Ln_B8G0MTUGWmIUlcCwCDPlVrzyxl4p74zSl_eo7B5DK
sA4Gp903s2BYCDBYyo7jbiYixyOJrsGSbMHgexlC6rTKTS1SmHzJjydVyaHWYvbD9dFGX8GsDZg
jLL65VpgwDJmVyDD75g4jyU6_LKxgFcONEO2SZbqomhV3ms6gH6P5wpsjxU1KPM5WiUcq4v9-
x1ByDg4CxZR37g9ZU50Qxlfrg1VEiPl5DG9yqBA7moEblpxVRymm1544dlp8DWW-
6fPMHck7VZuYy1SfRlGAbpJrgel7wuE-KMh0up3dQY6Lge--
okAIp_U17rO1Ty2bR_ZKCqynqWG41kQSlZiRlRsX6tq72yF1JZEXiG4mKnhTtX1banubKhZ4w-
```



شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

LrJOVKOeTox6q4abAMK6qmLVKlAli6r6yyQOXMnSxz6H\_gTpPVAOCGHJSI3BULk6AkzJW8UV51O  
SmkVrzuZLatPH1tiUDhDvWiiCJrOMkCNaeFyIOsdWoPjS2ldr1TLgO9v4-RSThM

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

li9QStJ6DuqnU\_v

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:

-aQ104fVd\_Cde3bcGt93TaVrcw93J7OMTODI3Hd3hsr3wu8fyDUh6LMb7OSM-  
APs10YlucelIu918515S\_V58xZm0mUm-  
ic4p7JvQX9dWbfzWOTZAKzqlFmRPFWOhbQYBXZ10Yu8Wht8tYHP26pzzbzxHhYbF6pLUziSTOn  
uYgRJUAhgflkTR8gzJzZ4K4laW2W8AKL5TFULU1PNavRMJ1IiaxHKZA-pL13Z-  
7XmuWyXnlvA4hTh-QUYEizaif-tSuEcOJTT6WVW\_dw\_825z7p3-jlljzae2b8KY6zMFNCJ-  
siXUq6syUz\_EYdtW2T3JidaugdS7hAlabTgRMEwg3QATQb071832IaF6DdlSv4NX1lXD-  
DY9fibtn07z1OzQ-qN-  
swh278dJmFPPaVv0mqzncZlpwYT0Y4cVlZ8fE4SVxsqgBNA9NmxUwe1BpIAxAcDbRLaKzSMxWrs  
KURwSHldPPiFQKGhQ4ScyiyiHmwRUzR4Yft9Dqsd-  
loI5Jrrj9hW4vVQT0KJ8rPLwLRhEcXjMYLeY5MHfJOoPZ3ivr7aqvKLS7goFHBVgO5X0zSvM3rN  
hmd1nK\_gHntzm-8QtXiIIKAXAq3zkW48i9FQup9SBWvStWr6-OZqN5CZl3dUNBALChq-  
neADAmzPudAXWarzxYtR6P3-WVcfsggofkHI8BYbVKCFrsSd8kpV\_Km7CqNLRP-  
L7fg8KIV0cyAN64WlaKqmzzj0d5e3frgatHTWtWuTKcm9\_zqKNd7pYaB6ufzgTpeVlOjEDq-  
HXHfGJV2QW9Q\_6-OpXuuF-aIkxWmeILsuJEGRBWuDb7aDznldUyQybmpoVQdNiiit-zymeMKHj-  
OnfSby\_pol6vSKFS2Af\_F0T5Pa2V5gPE5f-  
vuf1Ap\_NXRvVoznm4QhVPexbfIOSUTRmv74hF3Man5tB6AAOY7sDnigrJCRvA5q\_F5jV-kdZOB-  
v7f4RG4aEqOx6HuzmFTpdceQ0WuO--1NztUatv6OCau-  
dsnJdrZX6CW2GqoVY9E1X\_EKJLqUxeNjcn7UOBwaE514Qz8zHeIRJyo9U0dHV9VqSb0KFKKSoMO  
PXX4GQM3bNxcFiAgPH7I6ngBPYbAp0HjxhwkAsxWsUjEnvk2rmoA7aw\_70g76HuTASZgbXLArwQ



شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

pYl8dEPIk9Kxw8X3\_35wklxuSyQEzCyh-  
 k0r6hyE0IUQKRjP8IDfGHnaOdA2rf3ZQ8MrVpVAiwdTVt3y7q5rVGe-0E2DoKY-  
 RSRhz1qLWPopY88giG9pKyyCWGo6rf8R0qL\_JogcJe9lKPjaVUceYD4HoOfoyhP9FFALSqAly34  
 VPzgbYk2x3wI2ub2BWA1CbnuYSRmwWt5Qb3-ALwG34EIJIldQ2UMGu-  
 FAsldjTyH9Q417hLNk\_SU\_UlanpXFwz1-  
 yZM2TPySIsz\_hGerbxgf6nkiaElrMPXL4sevc3mpBEGwnSAjKcWPayUJkfDdo4QGQwoiFflPROT  
 avG-Nr2hH44MCQgE3FiUbPDVaOuxqDKQt-  
 86vpimTCDvBeaWJZDb95SKl5i2\_PJpVLciFc8hQTkhk9f23paPcTQc0YePN0xRr1WNI8qh3Us0U  
 znCLu2jeK9xh2UWLjUbC2YbBbPffIrmZidPXy1NNVR6QY0Ot-hhi4RED6nmvMORfO-  
 fxOVyst0hM4AXIzwSTyEqwHPeeiQVlkDtCviphAz6kMJ5zCylAF0qWPvOGKDVcohfWrB1DCdaa7  
 YwMMWAVE6NT3oieSRA9aJRZ226Mqn1qLTFHJ8S\_b9pg0WDt287Sr4bTDtbUF9p78-UBm21-G-  
 \_sMwo6E0qk5\_X18NqEMCYU9kDCXgkedFu0lxd2a-  
 tw8dpow90cLWj0guDULweI7h7pXTzDS1RpOisQdQYxjrf30jJn2cqUAGGTvjX25LesUvR-  
 2DiO\_E\_vBTbh7UHztmwyMAWc-  
 EaYqr8\_1GLuzx5GMP4VkfAovpNe3zPytpW\_c\_AJECTigl71kbNzgannXeVheTeR3ql4yVdrBHUub  
 uwkKry2PvgLbg6RcSGYDKszZI74XtLVpjeflMjhBx8ILKl8YjBcPkp26YS738HxWISu7Z6juQ9  
 REA9CeyJLNYlyTO5YrchPLYcWfhAjz9ZkOqF2hWIwagMkYHOnRAEO-PeDqpnRDiwv9-  
 FMDcYADRkdol95gVeWa6\_9jTiZ6D9XC\_UhCyBv\_MJzxX\_4UYpU0Q0piQdd0UcHHNRoPfCu7zkPI  
 BRi9F4ECgK3897uju6YhtWJNv2tRTOx5WdVf1SgtmurZL2O1SqCc7bguGbauWS56t9ETU0H51IJ  
 aFZa\_suhrQzKSOUBURvP7tw6t0fJjsYcbEc6F8kTnc9Jh1QRDjtAAvBJZFdolXojuaUllQ2h9LL  
 efZ6KTCdxFUqHrCLOftjib2rl-\_0flWY\_Xip\_7m\_W2YJ8-  
 jTypTtfcWmWPNeWJf4PcFaOuDgM2q5DdGWr\_FGUERKJqbAeb7q9L42W0witr2IEQasgzQjVWeNj  
 ZagTx\_7Xftsecv2jeywp5Mml5NYsF0umVLHjsbYg\_Zat6Uv1k\_shP-  
 0fFR\_QMKUwagOL6uTPmDpHK6L72mqB1lvHqiXgGsixsffZw5tuPvOnE4OPGrftFXeZtApbnItkA  
 jUKWEbaQIDzwmzLMBCs6nXiDomLhumOHRJCQH\_LbZvzGbMRrR9JaUS2Iceho\_GGO\_Qznq-C-  
 1rzZlebICcY2bMX\_62dUn\_FjQKlaKbSVP74DKWHnvTUyHyaaJ5JDYjTgmQYs4VLZ3222WKtN5kW  
 \_NJyRoP-datAgqrPTsTTEBfxAHmxP0fk41-9wK-  
 RcCJnQcToeWjk7dX6iNQwPbh4sIdZJhiR6zNDUS8QWQExAtiVmPCkYKJS5E0izOcP7t2Slvh755  
 gXPZ2b4xZgIgtGEKMi6N\_uFclXkutKGmvaDSCiThJTeAgpSnfYNFBFPhfzhAcxgCuL2pP3hLgX0  
 oRUhJ8KUnd6HvZaCsGxejc5zqdPwedy7kaUtVT8LkFrru\_lOstBrnQIOc03R0J6OKyyz7urslJw  
 1hwycsyYN2H-deKAtwn4XvLu4Em1LuVBG3pU7ND9TZg2U5UF5-1DBBxhG15kNP-  
 bNHeW9Tao6CgA54Vqfztwb5az-f2fPttP\_ixSgkgdSbPsI8vQ-  
 xqD5F8N6sUqTwOfcDqDpNcaeL9dxerV7dmD\_4SpoItQ26ngXUbfywen3FX07INLt\_oQO1HCBVg  
 dIj5rltnuYw7Zs5L25ZERS7APgRyS7iqGJM2dCoryFBxobsFa77e\_Up5TJ3rd6xndn937pbzjGD  
 C59DhJXXWZn0SHajCLU\_msOs6CmyDaJgGTRLUjGO9hjvwC79a4GaYqC2-  
 Uy376eMwMeD694AZyB2f7YCK6bk3WpTgc5K2keaKWBRosM5kdfS-3\_coySmgW-  
 zWZ7rXmvwNyI0JKdhluizi5Sd2MxulUKeWIVZ1DyoJay9Xisx9csZpyLyTWocoSLbbKzPD2fue3  
 9E3h7KstXd9il\_WWovN5Ba5ytrOzIWEjASsS97Eb7vTpjOUSLO2Cg-  
 f8ODqlbfigDlwUsna5IrrmGxbIf\_pLlG8FHMZRzRW\_jnvXn8oMapA



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

C5tP-5LuAdVN-wJ85igtXw

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:

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIiwia2lkIjoieNmEyYmNkO  
DgtYTg3MS00MjQ1LWEzOTMtMjg0M2VhZmU2ZTAyIn0.XUalz2m2Shs7hQut3eHYAgasxvw7\_Z4A  
F6H3fenBXPA\_pPz5u9P2v9LkiC-  
Qcqy4ADoJcvitpBLuxhvMMp7y8u8tklDV0ALsOYwqsZ2N8ew4oeTy69seeOT0kLeZBcUySkhBs3  
FnrkXa0U84XcqWnUypOixKEYH5qG96Ln\_B8G0MTUGWmiUlcCwCDPlVrzyxlc4p74zSl\_eo7B5DK  
sA4Gp903s2BYCDBYyo7jbiYixyOJrsGSbMHgexlC6rTKTS1SmHzJjydVyaHWYvbD9dFGX8GsDZg  
jLL65VpgwDjMvyDD75g4jyU6\_LKxgFcONE02SZbqomhV3ms6gH6P5wpsjxU1KPM5WiUcq4v9-  
x1ByDg4CxZR37g9ZU50Qxlfrg1VEiPl5DG9yqBA7moEblpxVRymm1544dlp8DWw-  
6fPMHck7VZuYy1SfRlGAbpJrgeL7wuE-KMh0up3dQY6Lge--  
okAIP\_U17r01Ty2bR\_ZKcqynqWG41kQSlZiRlRsX6tq72yF1JZEXiG4mKnhTtX1banubKhZ4w-  
LrJOVKOETox6q4abAMK6qmLVK1Ali6r6yyQOXMnSxz6H\_gTpPVAOCGHJSI3BULk6AkzJW8UV510  
SmkVrzuZLatPH1tiUDhDvWiicJrOmKCNaeFyIOSdWoPjS2ldr1TLgO9v4-  
RSThM.li9QSJtJ6DuqnU\_V.-  
aQ104fVd\_Cde3bcGt93TaVrcw93J7OMTODI3Hd3hsr3wu8fyDUh6LMb7OSM-  
APs10YlucelIu918515S\_V58xZm0mUm-  
ic4p7JvQX9dWbfzWOTZAKzqlFmRPFWOhbQYBXZ10Yu8Wht8tYHP26pzbzxHhYbF6pLUziSTOn  
uYgRJUAhgflkTR8gzJzZ4K4laW2W8AKL5TFULU1PNavRMJ1IiaxHKZA-pL13Z-  
7XmuWyXnlvA4hTh-QUYEizaif-tSuEcOJTT6WVW\_dw\_825z7p3-jlljzae2b8KY6zMFNcJ-  
siXUq6syUz\_EYdtW2T3JidaugdS7hAlabTgRMEwg3QATQb071832IaF6DdlSv4NX11XD-  
DY9fibtn07z1ozQ-qN-  
swh278dJmFPaVv0mqzncZlpwYT0Y4cVlZ8fE4SVxsqgBNA9NmxUwelBpIAXAcDbRLaKzSMxWrs  
KURwSHldPPiFQKGhQ4ScyiyiHmwRUzR4Yft9Dqsd-  
loI5Jrrj9hW4vVQT0KJ8rPLwlRhEcXjMYLeY5MHfJ0oPZ3ivr7aqvkLS7goFHBVgO5X0zSvM3rN  
hmDlnK\_gHNTzm-8QtxiI1KAXAq3zkW48i9FQup9SBWvStWr6-OZqN5CZ13dUNBALChq-  
neADAmzPudAXWarzXyTr6P3-WVcfsggofkHI8BYbVKCfrsSd8kpV\_Km7CqNLRP-  
L7fg8KIV0cyAN64WlaKqmmzzj0d5e3frgatHTWtWuTKcm9\_zqKNd7pYaB6ufzgtPeVl0jEDq-  
HXHfGJV2QW9Q\_6-OpXuuF-aIkxWmeILsuJEGRBwuDb7aDznldUyQybipoVQdNiit-zymeMKhj-  
OnfSby\_pol6vSKFS2Af\_F0T5Pa2V5gPE5f-  
vuf1Ap\_NXRvVoznm4QhVPexbfIOSUTRmv74hF3Man5tB6AAOY7sDnigrJCRvA5q\_F5jV-kdZOB-  
v7f4RG4aEqOx6HuzmFTpdceQ0WuO--1NztUatv6OCau-  
dsnjdrZX6C2GqoVY9E1X\_EKJLqUxeNjcn7UOBwaE514Qz8zHeIRJyo9U0dHV9VqSb0KFKKSoMO  
PXX4GQM3bNxcFiAgPH7I6ngBPYbAp0HjxhwkAsxWsUjEnvk2rmoA7aw\_70g76HuTASZgbXLArwQ  
pY18dEPIk9Kxw8X3\_35wklxuSyQEZYCyh-  
k0r6hyE0IUQKRjP8IDfGHnaOdA2rf3ZQ8MrVpVAiwdTVt3y7q5rVGe-0E2DoKY-  
RSRhZlqLWPpY88giG9pKyyCWGo6rf8R0qL\_JogcJe9lKPjaVUceYD4HoOfoyhP9FFALSqAly34  
VPzgbYk2x3wI2ub2BWA1CbnuYSRmwWt5Qb3-ALwG34EIJiIdQ2UMGu-  
FASldjTyH9Q417hLNk\_SU\_UlanpXFwz1-  
yZM2TPySIsz\_hGerbxgf6nkiaElrMPXL4sevc3mpBEGwnSAjKcWPAYUJkFDdo4QGQwoiFflPROT  
avG-Nr2hH44MCQgE3FiUbPDVaOuxqDKQt-  
86vpimTCDvBeaWJZDb95SK15i2\_PjPVLciFc8hQTkhk9f23paPcTQc0YePN0xRr1WNi8qh3UsOU  
znCLu2jeK9xh2UWLjUbC2YbBbPfFirmZidPXy1NNVR6QY00t-hhi4RED6nmvMORfO-  
fxOVyst0hM4AXIzwSTyEqwHPeeiQVlkDtCviphAz6kMJ5zCylAF0qWPvOGKDvCohfWrB1DCdaa7  
YwMMWAVE6NT3oieSRA9aJRZ226Mqn1qLTFHJ8S\_b9pg0WDt287Sr4bTDtbUF9p78-UBm21-G-  
\_sMwo6E0qk5\_X18NqEMCYU9kDCXgkedFuOlxd2a-  
tw8dpow90cLWj0guDULweI7h7pXTzDS1RpOisQdQYxjrf30jJn2cqUAGGTvjX25LesUvR-  
2DiO\_E\_vBTbh7UHztmwyMAWc-  
EaYqr8\_1GLuzx5GMP4VkfAovpNe3zPYtpW\_c\_AJECTigl7lkbNzggnXevHeTeR3ql4yVdrBHUub  
uwkKry2PvgLbg6RcSGYDKszZI74XtLVpjeflMjhBx8ILK18YjBcPkp26YS738HxWISuD7Z6juQ9  
REA9CeyJLNYlyTO5YrchPLYCwfhAjz9ZkOqF2hWIwagMkYHONRAEO-PeDqpnRDIwv9-  
FMDcYADRkDol95gVeWa6\_9jTiZ6D9XC\_UhCyBv\_MJzx4\_4UYpU0Q0piQdd0UcHNNR0PfCu7zkPI  
BRI9F4ECgK3897uju6YhtWJNv2tRTOx5WdVf1SgtmurZL201SqCc7bguGbauWS56t9ETU0H51IJ  
aFZa\_suhrQzKSOUBURvP7tw6t0fJjsYcbEc6F8kTnc9Jh1QRDjtAAvBJZFdo1XojuaU1lQ2h9LL  
efZ6KTCdxFUqHrCLOftjib2rl-\_0flWY\_Xip\_7m\_W2YJ8-  
jTypTtfcWmWPNeWJf4PcFaOuDgM2q5DdGWr\_FGUERKJqbAeb7q9L42W0witr2IEQasgzQjVWENj

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

ZagTx\_7Xftsecv2jeywp5Mml5NYsF0umVLHjsbYg\_Zat6Uv1k\_shP-  
0fFR\_QMKUwagOL6uTPmDpHK6L72mqB1lvHqiXgGsixsfFZw5tuPvOnE4OPGrftFXeZtApbnItkA  
jUKWEBaQIDzwmzLMBCs6nXiDOmLhumOHRJCQH\_LbZvzGbMRrR9JaUS2Iceho\_GGO\_Qznq-C-  
1rzZlebICcY2bMX\_62dUn\_FjQKlaKbSVP74DKWHnvTUyHyaaj5JDyJtgmQYs4VLZ3222WktN5kW  
\_NJyRoP-datAgqrPTsTTEBfxAHmxP0fk4l-9wK-  
RcCJnQcToeWjk7dX6iNQwPbh4sIdZJhiR6zNDUS8QWQExAtiVmPCkYKJS5E0izOcP7t2Slvh755  
gXPZ2b4xZgIgtGEKMi6N\_\_uFclXkutKGmvaDSCiHJTeAgpSnfYNFBFPhfzhAcxgCuL2pP3hLgX0  
oRUhJ8KUnd6HvZaCsGxejc5zqdPwedy7kaUtVT8LkFrru\_lOstBrnQIOc03R0J6OKyzz7urslJw  
1hwcysyYN2H-deKAtwn4XvLu4Em1LuVBG3pU7ND9TZg2U5UF5-lDBBxhG15kNP-  
bNHeW9Tao6CgA54Vqfztwb5az-f2fPttP\_iXsGkgdSbPsI8vQ-  
xqD5F8N6sUqTwOfcDqDpNcaeL9dxerV7dmD\_4SpoItQ26ngXUbfywen3FXO7INLt\_oQO1HCMVBG  
dIj5rltnuYw7Zs5L25ZERS7APgRyS7iqGJM2dCoryFBxobsFa77e\_Up5TJ3rd6xndn937pbzjGD  
C59DhJXXWZn0SHajCLU\_msOs6CmyDaJgGTRLUjGO9hjvwc79a4GaYqC2-  
Uy376eMwMed694AZYB2f7YCK6bk3WpTgc5K2keaKWBRosM5kdfS-3\_coySmgW-  
zWZ7rXmvwNyI0JKdhluizi5Sd2MxulUKeWIVZ1DyoJay9Xisx9csZpyLyTWocoSLbbKzPD2fue3  
9E3h7KstXd9il\_WWovN5Ba5ytrOzIWEjASsS97Eb7vTpjOUSLO2Cg-  
f8ODqlbfigDlwUsna5IrrmGxbIf\_pLlG8FHMZRwRW\_jnvXn8oMapA.C5tP-5LuAdVN-  
wJ85igtwxw

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 صورت حساب 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 }";

```

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

```

/** 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("typ", "jose");
jws.setHeader("crit", new String[]{"sigT"});
jws.setContentTypeHeaderValue("text/plain");

jws.sign();

String signedJson = jws.getCompactSerialization();

/** 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 ی امضا شده و رمز شده ی صورت حساب می باشد. در این بخش هم برای عملیات تولید JWS و JWE از کتابخانه jose-4 نسخه 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

```

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

```

{
    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 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("typ", "jose")
            .AddHeader("crit", new[] { "sigT" })
            .AddHeader("cty", "text/plain")
            .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);
    }
}

```



شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

```

}
}

```

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

```

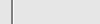
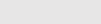
<PackageReference Include="jose-jwt" Version="4.1.0" />
<PackageReference Include="JWT" Version="10.0.2" />
<PackageReference Include="System.Security.Cryptography.Cng"
Version="6.0.0-preview.4.21253.7" />
<PackageReference Include="System.Security.Cryptography.X509Certificates"
Version="4.3.2" />
<PackageReference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

Send Invoices – ارسال صورتحساب	
آدرس	<a href="https://tp.tax.gov.ir/requestsmanager/api/v2/invoice">https://tp.tax.gov.ir/requestsmanager/api/v2/invoice</a>
Method	POST
ورودی	<p>لیستی از InvoicePacket ها هر یک شامل موارد زیر:</p> <ul style="list-style-type: none"> <li>header: آبجکت Json <ul style="list-style-type: none"> <li>requestTraceId: شناسه منحصر به فرد درخواست از نوع uuid</li> <li>fiscalId: از نوع رشته، شناسه حافظه صادرکننده‌ی صورتحساب</li> </ul> </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 حداکثر ۱۰۰۰ صورتحساب وجود دارد.</p>
خروجی	<p>آبجکت Json دارای فیلدهای زیر:</p> <ul style="list-style-type: none"> <li>timestamp: برچسب زمانی لحظه ایجاد جواب</li> <li>result: آرایه‌ی Json هر یک شامل شیئی که دارای فیلدهای زیر است: <ul style="list-style-type: none"> <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> </ul> </li> </ul>

شناسه سند RC_TICS.IS_v1.3	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
مهر ۱۴۰۲		

- data: در اینجا null است.

با استفاده از این API شرکت معتمد می تواند همه ی صورتحساب های مودیان مختلفی که دسترسی ارسال صورتحساب را به شرکت معتمد واگذار کرده اند ارسال نماید و نیازی نیست همه ی 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 می‌شود. همچنین در صورتی که ارسال کننده درخواست برای یک شناسه یکتا برای دو صورتحساب از `requestTraceId`های تکراری استفاده نماید هنگام استعلام وضعیت صورتحساب با `uid` تنها پاسخ وضعیت یکی از آن‌ها به عنوان جواب برگردانده می‌شود.



نمونه درخواست cURL ارسال صورت حساب و پاسخ آن:

```
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 ]...EEZe9mxIiw",
  "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
    }
  ]
}
```



شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

] }  
}

## ۸ - استعلام وضعیت صورتحساب‌های ارسالی

پس از تولید یک بسته صورتحساب امضا شده و رمز شده 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 تولید شده توسط خودتان) و یا از طریق زمان ارسال صورتحساب می‌توانید نسبت به وضعیت پردازش صورتحساب و خطاهای احتمالی موجود در آن مطلع شوید. به عنوان مثال فرض کنید خروجی درخواست ارسال دو صورتحساب به شکل زیر می‌باشد:



```
{
  "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.

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

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



Inquiry by Reference Id - استعلام به وسیله شماره پیگیری	
<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>	آدرس
GET	Method

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

<p>فیلدهای زیر:</p> <ul style="list-style-type: none"> <li>referenceIds: لیست شماره‌ی پیگیری‌هایی که قرار است اعلام 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 اعلام نمی‌تواند از یک هفته بیشتر باشد.</p> <p>محل قرارگیری: Request Params</p>	ورودی
<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"> <li>referenceNumber: شماره پیگیری درخواست اعلام شده</li> <li>uid: شناسه درخواست (همان requestTraceId که صورتحساب با آن ارسال شده بود)</li> <li>status: وضعیت صورتحساب دارای حالت‌های زیر: <ul style="list-style-type: none"> <li>SUCCESS: صورتحساب فاقد خطا بود و با موفقیت در کارپوشه ثبت شد.</li> <li>FAILED: صورتحساب ارسالی دارای خطا بوده و رد شده است.</li> <li>PENDING: صورتحساب ارسالی هنوز در صف بررسی می‌باشد.</li> <li>NOT_FOUND: شماره پیگیری داده شده یافت نشد.</li> </ul> </li> <li>data: لیست خطاها / اخطارهای موجود در صورتحساب</li> <li>packetType: نوع بسته</li> <li>fiscalId: شناسه حافظه ارسال‌کننده‌ی صورتحساب</li> </ul>	خروجی

نمونه درخواست اعلام 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%3A00.000000000%2B03%3A30&end=2023-05-
```

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

```
14T21%3A00%3A00.000000000%2B03%3A30' \
-H 'accept: */*' \
-H 'Authorization: Bearer eyJhbGciOi...[ JWT TOKEN ]...q4RcXogA'
```

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



```
[
  {
    "referenceNumber": "93367b02-23dd-4568-90e1-2b47d799f361",
    "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": "A11216"
  },
  {
    "referenceNumber": "f9173085-2316-4ca6-918e-e41aaf7ef8dd",
    "uid": "c5352f85-9322-41bc-a5b2-9abb130fe622",
    "status": "SUCCESS",
    "data": {
      "error": [],
      "warning": [],
      "success": true
    },
    "packetType": "receive_invoice_confirm",
    "fiscalId": "A11216"
  }
]
```

همانطور که می بینید یکی از صورت حساب ها با موفقیت ثبت شده و هیچ خطا و اختطاری ندارد. ولی یکی از صورت حساب ها دارای خطا بوده و خطای موجود در آن در قسمت error قابل مشاهده می باشد.

## ۸-۲- اعلام با uid

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

### Inquiry by uid – اعلام به وسیله شناسه درخواست

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		



آدرس	<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>
Method	GET
ورودی	<p>فیلدهای زیر:</p> <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> <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>
خروجی	دقیقا مانند استعلام با شماره پیگیری

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": "011107",
          "message": "شناسه/ملی شناسه/شماره «فیلد در شده وارد مقدار طول»  
مقدار طول) . است مجاز طول حداکثر از بزرگتر «خریدار فراگیر کد/مدنی مشارکت  
(باشد 10 حداکثر باید شده وارد",
          "errorType": "ERROR"
        }
      ]
    },
    "warning": [
```

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

```

{
  "code": "111208",
  "message": "«خریدار اقتصادی شماره» فیلد در شده وارد مقدار طول",
  "(باشد 14 حداقل باید شده وارد مقدار طول) . است مجاز طول حداقل از کوچکتر",
  "errorType": "WARNING"
},
{
  "success": false
},
{
  "packetType": "receive_invoice_confirm",
  "fiscalId": "A111YO"
},
{
  "referenceNumber": "60e834f9-14b6-43be-8b77-85471678d3da",
  "uid": "cb080c58-e36f-4bb0-a932-90f672109fb6",
  "status": "SUCCESS",
  "data": {
    "error": [],
    "warning": [],
    "success": true
  },
  "packetType": "receive_invoice_confirm",
  "fiscalId": "A111YO"
}
]



```

همانطور که مشاهده می کنید، یکی از صورتحساب ها با موفقیت در کارپوشه ثبت شده و دیگری دارای خطا می باشد و لیست خطاها و هشدارهای موجود در صورتحساب برگردانده می شوند.

### ۸-۳- اعلام براساس بازه زمانی

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

Inquiry - اعلام در بازه زمانی	
آدرس	<a href="https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry">https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry</a>
Method	GET
ورودی	<p>فیلدهای زیر:</p> <ul style="list-style-type: none"> <li>• pageNumber: شماره صفحه (مقدار پیش فرض: ۱)</li> <li>• pageSize: اندازه ی صفحه (مقدار پیش فرض: ۱۰ - مقادیر مجاز: ۱ تا ۱۰۰)</li> <li>• status: وضعیت صورتحساب هایی که به دنبال آن هستیم.</li> </ul> <p>○ مقادیر مجاز: SUCCESS, FAILED, TIMEOUT, PENDING</p>

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		



<p>○ در صورتی که این فیلد خالی باشد تمامی صورتحساب‌ها برگردانده می‌شود.</p> <ul style="list-style-type: none"> <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.</p> <p>محل قرارگیری: Request Params</p>	
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:

```
[
  {
    "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 (مقدار طول) . است مجاز طول حداکثر از بزرگتر «خریدار فراگیر کد/مدنی مشارکت (باشد 10 حداکثر باید شده وارد",
          "errorType": "ERROR"
        }
      ],
      "warning": [
        {
          "code": "111208",
          "message": "«خریدار اقتصادی شماره» فیلد در شده وارد مقدار طول (مقدار طول) . است مجاز طول حداقل از کوچکتر (باشد 14 حداقل باید شده وارد مقدار طول)",
          "errorType": "WARNING"
        }
      ],
      "success": false
    },
    "packetType": "receive_invoice_confirm",
  }
]
```

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

```

    "fiscalId": "A111YO"
  },
  {
    "referenceNumber": "60e834f9-14b6-43be-8b77-85471678d3da",
    "uid": "cb080c58-e36f-4bb0-a932-90f672109fb6",
    "status": "SUCCESS",
    "data": {
      "error": [],
      "warning": [],
      "success": true
    },
    "packetType": "receive_invoice_confirm",
    "fiscalId": "A111YO"
  }
]

```

## 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"> <li>memoryId: شناسه حافظه مورد نظر</li> <li>محل قرار گیری: Request Params</li> </ul>
خروجی	شیء JSON شامل فیلدهای زیر: <ul style="list-style-type: none"> <li>nameTrade: شناسه حافظه</li> <li>fiscalStatus: وضعیت حافظه</li> <li>saleTreshold: حد مجاز فروش پرونده</li> <li>economicCode: کد اقتصادی پرونده</li> </ul>

نمونه ورودی:

```

curl -X 'GET' \
  'https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information?memoryId=A11216' \

```

شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

```
-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",
  "saleThreshold": null,
  "economicCode": "14003778990"
}
```

## ۹-۲- اطلاعات مودی



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

GET Taxpayer – دریافت اطلاعات مودی	
<a href="https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer">https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer</a>	آدرس
GET	Method
<ul style="list-style-type: none"> <li>economicCode: شماره اقتصادی مودی</li> </ul>	ورودی
<p>محل قرار گیری: Request Params</p> <p>شیء JSON شامل فیلدهای زیر:</p> <ul style="list-style-type: none"> <li>nameTrade: نام مودی / پرونده اقتصادی</li> <li>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 غیرمجاز موقت، «PERMANENT_UNAUTHORIZE» به معنی غیرمجاز دائم و «ARTICLE_2_SUBJECT» به معنی مشمول تبصره ماده ۲ می باشد.</li> <li>nationalId: شناسه ی ملی پرونده</li> </ul>	خروجی

نمونه درخواست ارسالی:



```
curl -X 'GET' \
'https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer?economicCode=14003778990' \
-H 'accept: */*' \
-H 'Authorization: Bearer eyJhbGci...[ JWT Token ]...klQXOM-_uA'
```



شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

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 «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

## ۱۰- پیوست‌ها



### ۱۰-۱- جدول خطاها و کدهای وب سرویس جمع آوری

در صورتی که ورودی‌های درخواست به درستی و در ساختار صحیح به API های وب سرویس جمع آوری داده شوند و مشکلی در فرآیند اجرای درخواست و دسترسی‌ها وجود نداشته باشد درخواست انجام شده و خروجی به فرمی که در سند گفته شد برگردانده می‌شود. ولی در صورتی که در داده‌های ورودی، دسترسی‌ها و یا فرآیند اجرای عملیات مربوطه مشکلی به وجود بیاید، API خطاهای رخ داده را با ساختار زیر برمی‌گرداند:

```
{
  "timestamp": 1687772718290,
  "requestTraceId": "string",
  "errors": [
    {
      "code": "string",
      "message": "string"
    }
  ]
}
```

timestamp برچسب زمانی رخداد خطا به فرمت Epoch می‌باشد. requestTraceId کد شناسایی درخواست است که می‌تواند برای رهگیری مراحل رخداد خطا استفاده شود. errors لیستی از خطاهای رخ داده می‌باشد که هر یک دارای code و message می‌باشند. در جدول زیر لیست کدها و پیغام‌های زیرسامانه جمع آوری و محل رخداد هر کدام را می‌توانید ببینید:

جدول خطاهای احراز هویت درخواست		
پیغام	Http Status	کد خطا
(در صورت نفرستادن توکن Bearer در سرآیند درخواست این خطا بدون هیچ پیغامی نمایش داده می‌شود).	403	
ساختار payload در توکن JWT فرستاده شده مطابق با ساختار {"nonce":"string","clientId":"string"} نمی‌باشد.	401	۴۱۰۱
چالش تصادفی امضا شده در توکن JWT معتبر نمی‌باشد (قبلا استفاده شده یا زمان استفاده آن گذشته است).	401	۴۱۰۲



شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

کد ملی گواهی امضایی که توکن JWT با آن امضا شده با کد ملی مربوط به شناسه کلاینت قرار داده شده در توکن مطابقت ندارد.	401	۴۱۰۳
شناسه کلاینت (شناسه حافظه) وارد شده در توکن JWT یافت نشد.	401	۴۱۱۰
شناسه کلاینت (شناسه شرکت معتمد) وارد شده در توکن JWT یافت نشد.	401	۴۱۲۰
ساختار توکن JWT فرستاده شده صحیح نیست.	401	۴۱۳۰
امضای توکن JWT یا گواهی امضای فرستاده شده معتبر نمی باشد.	401	۴۱۳۱
زمان اعتبار چالش تصادفی باید بین ۱۰ تا ۲۰۰ ثانیه باشد.	400	۴۱۴۶
مشکل غیرمنتظره در دریافت اطلاعات پرونده مالیاتی رخ داد.	500	۵۱۱۹
مشکل غیرمنتظره در دریافت اطلاعات شرکت معتمد رخ داد.	500	۵۱۲۹
خطای غیرمنتظره‌ای در بررسی صحت امضای توکن JWT رخ داد.	500	۵۱۳۹

در صورت رخدادن خطای غیر منتظره در هر یک از مراحل (خطاهایی که با ۵ شروع می شوند)، اگر نسبت به صحت ساختار درخواست ارسالی و پارامترهای ورودی و توکن Jwt مطمئن هستید، می توانید مدتی صبر کنید و مجدداً درخواست خود را ارسال نمایید.

جدول خطاهای فراخوانی API ارسال صورتحساب		
پیغام	Http Status	کد خطا
در یک درخواست نمی توانید بیشتر از ۱۰۰۰ صورتحساب ارسال نمایید.	400	۴۱۴۳
بدنه‌ی درخواست ارسالی خالی است یا از نظر ساختار JSON معتبر نیست.	400	۴۱۴۴
در بدنه‌ی درخواست ارسالی، بعضی از فیلدهای ضروری خالی است (برای هر صورتحساب باید payload, requestTraceId و fiscalId موجود باشد).	400	۴۱۴۵
شناسه درخواست (requestTraceId) داخل درخواست معتبر نمی باشد.	400	۴۱۶۲
در درخواست ارسالی شناسه درخواست تکراری وجود دارد.	400	۴۱۶۳

جدول خطاهای فراخوانی API استعلام صورتحساب		
پیغام	Http Status	کد خطا
زمان شروع بازه‌ی استعلام باید قبل از زمان پایان آن باشد.	400	۴۱۴۰



شناسه سند	سند «دستورالعمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

نمی‌توانید در یک درخواست وضعیت بیش از ۱۰۰ صورتحساب را استعلام بگیرید.	400	۴۱۴۱
مقدار status وارد شده نامعتبر است. مقادیر مجاز: [ SUCCESS, FAILED, [PENDING, TIMEOUT]	400	۴۱۴۲
بازه زمانی استعلام حداکثر یک هفته است.	400	۴۱۶۴

جدول سایر خطاهای جمع‌آوری			
محل رخداد	پیغام	Http Status	کد خطا
در هر API	خطای غیر منتظره‌ای در انجام درخواست رخ داد.	500	۵۱۹۹
در هر API	فرمت ورودی‌های درخواست نادرست می‌باشد.	400	۴۱۴۷
اطلاعات حافظه	دسترسی مشاهده اطلاعات شناسه یکتای درخواست شده ممکن نیست.	403	۴۱۶۰
اطلاعات حافظه	شناسه یکتای درخواست شده یافت نشد/غیرفعال می‌باشد.	404	۴۱۶۱
اطلاعات مودی	شماره اقتصادی وارد شده یافت نشد.	404	۴۱۷۰

همچنین در صورت وجود خطا در ساختار امضا و رمزگذاری صورتحساب (بسته‌ی JWE و JWS) یا وجود خطا در دسترسی‌های صدور و ارسال صورتحساب، هنگام استعلام وضعیت صورتحساب خطاهای زیر با همان فرمت ذکر شده در پاسخ به استعلام وضعیت صورتحساب برگردانده می‌شوند:

خطاهای وب‌سرویس جمع‌آوری هنگام استعلام وضعیت صورتحساب	
پیغام	کد خطا
قرارداد شناسه یکتا و شرکت معتمد یافت نشد.	۰۴۱۱۱
ساختار بسته‌ی صورتحساب (encrypted payload) امضا شده صحیح نیست.	۰۴۱۳۰
امضای صورتحساب ارسالی یا گواهی امضایی که صورتحساب با آن امضا شده معتبر نمی‌باشد.	۰۴۱۳۱
گواهی امضایی که صورتحساب با آن امضا شده، دسترسی صدور و امضای صورتحساب برای این شناسه یکتا را ندارد.	۰۴۱۳۲
شناسه حافظه امضا کننده‌ی صورتحساب یافت نشد/غیرفعال می‌باشد.	۰۴۱۳۳
شناسه شرکت معتمد امضا کننده‌ی صورتحساب یافت نشد/غیرفعال می‌باشد.	۰۴۱۳۴

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

بسته ی JWE صورت حساب ارسالی از نظر ساختاری معتبر نمی باشد و امکان رمز گشایی آن وجود ندارد.	۰۴۱۵۰
خطای غیر منتظره ای در فرآیند بررسی امضای صورت حساب رخ داد.	۰۵۱۳۹
خطایی غیر منتظره در رمز گشایی صورت حساب ارسالی رخ داد.	۰۵۱۵۱

## ۱۰-۲- گواهی و کلید خصوصی امضا

گواهی امضایی که در Header بسته های Jws فرستاده می شود برابر است با:

-----BEGIN CERTIFICATE-----



MIIDejCCAmKgAwIBAgIUUV27QXqJjK2EgFy9zeYkpsX+ISPswDQYJKoZIhvcNAQEL  
BQAwcTELMAkGA1UEBhMCSVIxDDAKBgNVBAGMA1RlaDEMMAoGA1UEBwwDVGVomREw  
DwYDVQQKDAhNb2hhew11bjEMMAoGA1UECwwDVGF4MSUwIwYJKoZIhvcNAQkBFhZt  
Lm1hbHZlcmRpQG1vaGF5bWVuLm1yM4XDTIzMDMyNDEzMjgyM1oXDTI0MDMyMzEz  
MjgyM1owTTEPMA0GA1UEAwwGQW56YXpMRcwFQYDVQQKDA5RdW9WYWRpcyBHcm91  
cDELMAkGA1UEBhMCSVIxFDASBgNVBAUTCzE0MDAzNzc4OTkwMIIBIjANBgkqhkiG  
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzLgyk5K06+j9d1ud0i1JArrZ3Whw/w9wEzHB  
9yXwENRa5fm5AbRukMF5b6VGeKzD6LZuL9+tfdFfWypCjI++gGNyWzRmEHKpTnzP  
1t6NyuXKfm4nBVAb1sugSw8Y5DEXRfTqILgBWN/pZ4zGlifEALMcGAs7ADcjnv7b  
/tM2wxr9rHxsCvW4HvlzQask8Qr1CrKgT0EI66rSXCHep/uIONDWP0W20e1M1ZtM  
6AAjWXRLGcshPIHuK+ZLfAFxWtoGonf6qN9ypos2B18D/EFa8WHON62eYKT0kW3j  
BVA3yPEKRWkdDjDu/3CPzymhf3WfYwxb4t35oWb/qUXGVIvIDvIDvIDvIDvIDvIDv  
BgNVHSMEDAwgBSx+Oq+R03x/FmyCp+jcmfOH+Fn9TAJBgNVHRMEAjAAMA0GCSqG  
SIb3DQEBCwUAA4IBAQAQKATXlnS+pPtAiRIYGtydVU5Vi7Aq+D6QW07uFqcB7vBh  
ddN3yX21VVcwptNjzhv8UCM+mDMv1msRVKVtMoo5fHfII92/Wo8rUz1RP+yhyCk0  
Vz8I11v+bjLwVur/agC/s5Rf0m66pNNjFZ9J3S2N31ChXYWz2vvA8pdAYvWTu9g5  
u4FMFqlsaLwMGC+WA0g3KYzRkdWRy1vd23hLTUcVsWM8wpgZ11wEGE1khca/Sd0  
mCU2HG5vIbqFfTjA6to0fY07CE5fD8aR3UcXjNduosVO52ZqCX5SabrhFS3AGHFR  
jpFnI5LZespiCXSA8Sv3k0SCSRQKqFbiwSFM8Zjg

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

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

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

MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQMudKTko7r6P13  
W53SKUkCutndaHD/D3ATMcH3JfAQ1Fr1+bkBTg6QwX1vpUZ4rMPotm4v36190V9b  
I9yMj76AY3LDNGYQcq10fM/W3o3K5cp+bicFUBuWy6BLDXjkmRdF90oguAFY3+ln  
jMaWJ8QAsxwYCzsAnyOe/tv+0zbDGv2sfGwK9bge+XNBqwrxCvUKsqBPQQjrqtJc  
Id6n+4g40NanRbY56UyVm0zoACNZdEsZyyE8ge4r5kt8AXFa2gaid/qo33KmizYH  
XwP8QVrxYc43rZ5gpPSRbeMFVrfI8SRHCR00M07/cI/PKaf/dYVjdGLvi3fmhZv+  
pRcZUh2/AgMBAAECggEACPPC7YnNzram9ucDosXAt+ftyfHckrLgnVbfRLfBN8G4  
QsGSxWpeNub1Jmo/Due0p63oYx0SBKR75AlmKLV1CzhRPhI8L5h3qEN88dVMrosp  
OCYoe+kpbJF9dA0zcD5e40h+o/StynH3UF0yED+qLsWsA7nqWnYQj9ZpW2Fz01Z1

شناسه سند	سند «دستور العمل فنی اتصال به سامانه مودیان»	 
RC_TICS.IS_v1.3		
مهر ۱۴۰۲		

i5NRX4YgyIopHfqcLWJWpOR8n4HwDY18BL7tMi31f0sZXz56EUgBPxq5RMi+1iKW  
pyZdwy4TrJL/Sj4tWkKJ7ELVd47VunizAqeLDy8bL1PBX0PewRvR37P9axHLjsj/  
d1Iw/xvqgVEWZTyUXzg4qgFU5Na5u6xIW8JyqejdEQKBgQD2Q1DdoPOtG1URyuu0  
4HJlQ85ZFEWAA0vvp8esvJLJ7t73Rz28RkKAMHW/njr23ExxV3eek9J11GENJUZF  
KsNNTjRWMgCxUic00MGTJuraWHRema00YNNjpVd3pIi68p51CZNzMRLn2J8F+7CP  
eGiynKEvKU43KcJr6K0kWP14FQKBgQDU0T3SNr7af4y3r03ds2DMaoKEG531tuLu  
nrZNnL4a/i2r3AlI5K470UkmAXDD1kgGf235KxrRm7x7VVp5SZLgOPqgJ20KKk9b  
HLvuAdxCeUlndfJWrAmYcmYLLCSDHBudN/evF6WiNaQi074MhdbaxYdLiiXdS3VV  
f1Q/8m6/gwKBgD4ijXTeX52V/+j1YnDB8RtL+IzrpkMrocVeeCtFiwQa0Xf7KcCP  
mcfuckdfDVGSVD1k7HG+qqOwRKykCw6Qs6awCpSVGUekiuZaFf2jHC7r1E522BUX  
OT8zQNaXVUiWXXt4zzOLF1IZfkZsMyiAISqwCptzuKCCkOPZVzDoo0vhAoGBAMo8  
2XnVyoKLKwC2r4i600eo48S1FeP12yuVqXqR1FqEZ1RlMnGR1z1DAjdasRV5oVKD  
cDeTzdWZIIIE3uFWAJFJt80WUiNQ4ptbXtINWQ0DsT2PebggNTsUPH7UVytDJ0jiq  
gfZjC2TdgTAR1g3Cdk3J3mtbqeXlGmiXN2rZcIMPAoGADfTonaehrsnscUcH4Dgs  
qZdyZm9JRmoNyisLBmbGkTNxoY09Vm/03u3NMsohkjopt2ly38ZMYX14FyXKEKcI  
977r33JD9PxRcovqFhcPR3WuQrPf6ND3IX6eB5p8d7m6fmFYSe/0NhWoeH99a6/c  
csAr2hPMOb/R3GdRewkSGgQ=

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