

مرکز تنظیم مقررات نظام پایانه های فروشگاهی و سامانه مودیان

سند

«دستورالعمل فني اتصال به سامانه موديان»

شناسه سند: RC_TICS.IS_v1.4

بهمن ۱۴۰۳

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



مقدمه

زیرسامانه ی جمع آوری صورتحساب یکی از زیرسامانه های سامانه ی مودیان است که وظیفه ی دریافت صورتحساب، ارسال به هسته، گرفتن نتیجه اعتبارسنجی صورتحساب و ذخیره کردن آن و پاسخ به استعلام های صورتحساب های ارسالی از سمت مودی را برعهده دارد. این زیرسامانه دارای یک وبسرویس می باشد که تمامی درخواست ها از طریق این وبسرویس به سامانه ارسال شده و پاسخ داده می شوند. این وبسرویس در چهار چوب REST API پیاده سازی شده و فراخوانی آن نیاز مند احراز هویت مودی از طریق امضای دیجیتال می باشد.

در این سند منابع موجود در این وب سرویس و نحوه ی فراخوانی و پاسخ دهی هر کدام شرح داده خواهد شد و در نهایت در قالب یک مثال فرآیند اتصال به سامانه ی مودیان و ارسال صور تحساب به طور کامل انجام می گیرد.

تغییرات این سند نسبت به نسخهی قبلی

بخش مرتبط	عنوان تغيير	ردیف	
بخش ۱۰	اضافه شدن سرويس استعلام وضعيت صورتحساب در كارپوشه	1	

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

ىند «دىتورالعمل فنى اتصال به سامانه موديان »



فهرست مطالب

۴	۱ – تعاریف۱
	– ۲ دریافت شناسه یکتای حافظه مالیاتی
	۳ - مراحل ارسال صور تحساب و استعلام وضعیت آن
	– ۴ منابع در دسترس و کاربردهای هر کدام
	- دریافت چالش تصادفی و احراز هویت $-$ ۵
	۶ – دریافت اطلاعات سرور
١٨	۷ - ارسال صور تحساب
٣٣	۸ - استعلام وضعیت ارسال صور تحساب
۴۲	۹ – استعلام اطلاعات حافظه و مودی
**	۱۰ - استعلام وضعیت صور تحساب در کارپوشه
۴۵	۱۱ – پیوستها

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

ىند « دستورالعمل فنى اتصال به سامانه موديان »



۱ - تعاریف

تعریف	عنوان
فرآیندی که طی آن فرستنده پیام به وسیلهی یک کلید خصوصی، رشتهای به نام امضا	
تولید می کند و آن را در کنار اصل پیام برای گیرنده می فرستد. گیرنده با در اختیار	امضاي
داشتن كليد عمومي فرستنده مي تواند نسبت به اصالت فرستنده اطمينان حاصل كند و	ديجيتال'
مطمئن شود محتوای پیام در طول مسیر تغییری نکرده است.	
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	گواهی امضا ^۳
یا cer میباشد و برای بررسی صحت امضای بستههای ارسالی مورد استفاده قرار	
می گیرد.	
صورتحسابی است دارای شماره منحصر به فرد مالیاتی که اطلاعات مندرج در آن، در	
حافظه مالیاتی فروشنده ذخیره می شود. مشخصات و اقلام اطلاعاتی صورتحساب	
الكترونيكي، متناسب با نوع كسب و كار توسط سازمان تعيين و اعلام مي شود. در	صور تحساب
مواردی که از دستگاه کارتخوان بانکی یا درگاه پرداخت الکترونیکی به عنوان پایانه	الكترونيك
فروشگاهی استفاده می شود، رسید یا گزارش الکترونیکی پرداخت خرید صادره در	
حكم صور تحساب الكترونيكي است.	
شماره منحصر به فرد مشخص كننده يك صورتحساب شامل شناسه حافظه مالياتي	
صادر کننده صورتحساب، تاریخ صدور، سریال صورتحساب و یک رقم کنترلی برای	شماره مالياتي
جلوگیری از صدور شماره مالیاتیهای نامعتبر.	
شناسهی یکتایی که توسط سازمان اختصاص یافته می شود و مودی می تواند از طریق	شناسه يكتاي
کارپوشه آن را دریافت کند و از آن به منظور صدور صورتحساب استفاده می شود.	حافظه مالياتي

Digital Signature [†]

Digital Signature Certificate *

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فني اتصال به سامانه مودمان »



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 مودى
 - 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.

 $\frac{re}{re}$ این سند با هدف استفاده از نسخه دوم APIهای سامانه مودیان و جهت تسهیل در فرآیند ارسال صورتحساب و اتصال به سامانه مودیان منتشر شده است. در این نسخه قابلیت استفاده از گواهی امضاء برای احراز هویت و ارسال صورتحساب ایجاد شده است. لازم به ذکر است تا اطلاع ثانوی امکان استفاده از نسخه قبلی APIهای سامانه مودیان نیز فراهم می باشد که راهنمای استفاده از آن به پیوست این سند بارگذاری گردیده است.

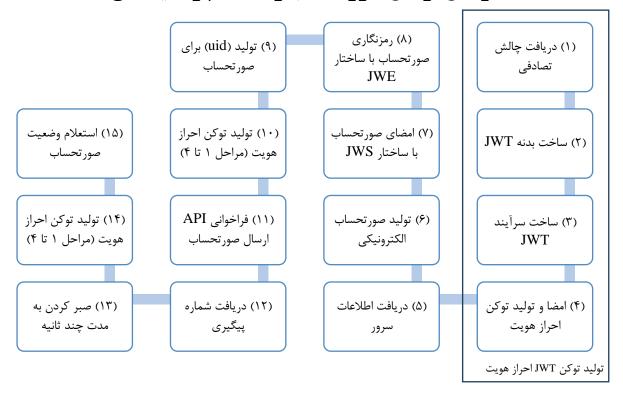
RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعل فني اتصال به سامانه مودبان »



۳ - مراحل ارسال صورتحساب و استعلام وضعیت آن



۴ - منابع در دسترس و کاربردهای هر کدام

وب سرویس جمع آوری سامانه ی مودیان در آدرس https://tp.tax.gov.ir/requestsmanager 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 همه ی منابع موجود در وبسرویس جمع آوری سامانه ی 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.

توضيحات	ساختار خروجي	درخواست	آدرس
دریافت چالش تصادفی راهنما در صفحه ۱۰	<pre>{ "nonce": "string", "expDate": "string" }</pre>	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/nonce?timeToLive=20' \ -H 'accept: */*'</pre>	GET https://tp.tax.gov.i r/requestsmanager /api/v2/nonce
ارسال صورتحساب راهنما در صفحه ۱۸	<pre>{ "timestamp": 0, "result": [</pre>	<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]EEzZe9mxIxw", "header": { "requestTraceId": "cf019c26-f235-11ed-a05b-0242ac120003", "fiscalId": "A11216" } } } }</pre>	POST https://tp.tax.gov.i r/requestsmanager /api/v2/invoice
دریافت اطلاعات پروندهی مودی راهنما در صفحه ۴۳	{ "nameTrade": "string", "taxpayerStatus": "string", "nationalId": "string" }	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer?economic Code=14003778990' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbG[JWT Token]klQXOuA'</pre>	GET https://tp.tax.gov.i r/requestsmanager /api/v2/taxpayer
دریافت اطلاعات حافظه راهنما در صفحه ۴۲	<pre>{ "nameTrade": "string", "fiscalStatus": "string", "nationalId": "string", "economicCode": "string" }</pre>	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal- information?memoryId=A11216' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGc[JWT Token]OFh9zw'</pre>	GET https://tp.tax.gov.i r/requestsmanager /api/v2/fiscal- information
دریافت اطلاعات سرور راهنما در صفحه ۱۷	<pre>{ "serverTime": 0, "publicKeys": [</pre>	<pre>curl -X 'GET' \ 'https://tp.tax.gov.ir/requestsmanager/api/v2/server- information' \ -H 'accept: */*' \ -H 'Authorization: Bearer eyJhbGci[JWT]Jv18fvHm0PKVA'</pre>	GET https://tp.tax.gov.i r/requestsmanager /api/v2/server- information

```
curl -X 'GET' \
                                                     'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-
                     "referenceNumber": "string",
                                                   reference-id?referenceIds=f9173085-2316-4ca6-918e-
                                                                                                                                  GET
استعلام صورتحساب با
                     "uid": "string",
                                                   e41aaf7ef8dd&referenceIds=93367b02-23dd-4568-90e1-
                                                                                                                             https://tp.tax.gov.i
                     "status": "string",
                     "data": {},
                                                   2b47d799f361&start=2023-05-
                                                                                                                             r/requestsmanager
                     "packetType": "string",
                                                   14T10%3A00%3A00.000000000%2B03%3A30&end=2023-05-
                                                                                                                              /api/v2/inquiry-
                     "fiscalId": "string",
راهنما در صفحه ۳۴
                                                   14T21%3A00%3A00.000000000%2B03%3A30'\
                                                                                                                              by-reference-id
                     "sign": "string"
                                                     -H 'accept: */*' \
                                                     -H 'Authorization: Bearer eyJhbGc...[ JWT TOKEN ]...q4RcXoqA'
                                                   curl -X 'GET' \
                                                     'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-
                     "referenceNumber": "string",
                                                   uid?uidList=cb080c58-e36f-4bb0-a932-
                                                                                                                                  GET
                     "uid": "string",
                                                   90f672109fb6&uidList=b3bd6327-1c57-4cae-85ed-
                                                                                                                             https://tp.tax.gov.i
                     "status": "string",
                                                   5c88de28aea3&fiscalId=A111Y0&start=2023-06-
                     "data": {},
                                                                                                                             r/requestsmanager
                     "packetType": "string",
                                                   10T00%3A00%3A00.000000000%2B03%3A30&end=2023-06-
                                                                                                                              /api/v2/inquiry-
                     "fiscalId": "string",
                                                   10T23%3A59%3A59.999999999%2B03%3A30'\
                                                                                                                                 by-uid
راهنما در صفحه ۳۷
                     "sign": "string"
                                                     -H 'accept: */*' \
                                                     -H 'Authorization: Bearer eyJhbGciO...[JWT TOKEN]...ski8e-A'
                                                   curl -X 'GET' \
                     "referenceNumber": "string",
استعلام براساس بازه
                     "uid": "string",
                                                   'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry?start=202
                                                                                                                                  GET
                     "status": "string",
                                                   3-06-10T00%3A00%3A00.00000000%2B03%3A30&end=2023-06-
                                                                                                                             https://tp.tax.gov.i
                     "data": {},
                                                   10T23%3A59%3A59.999999999%2B03%3A30&pageNumber=1&pageSize=10' \
                                                                                                                             r/requestsmanager
                     "packetType": "string",
                                                     -H 'accept: */*' \
                                                                                                                              /api/v2/inquiry
                     "fiscalId": "string",
راهنما در صفحه ۴۰
                     "sign": "string"
                                                     -H 'Authorization: Bearer eyJhbGci...[JWT TOKEN]...KXzBjRZw'
                   "taxId": "
                 A111DW04E8300004349008",
                                                   curl -X 'GET' \
                  "invoiceStatus": "APPROVED",
                                                     'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-
                 "article6Status":
                 "NOT EXCEEDED",
                                                   invoice-
                                                                                                                                  GET
                  "error": null
                                                   status?taxIds=A111DW04E8300004349008&taxIds=A111DW04E8300003CC4
                                                                                                                             https://tp.tax.gov.i
                                                   EA5' \
                                                                                                                             r/requestsmanager
                  "taxId":
                                                     -H 'accept: */*' \
                                                                                                                              /api/v2/inquiry-
                 "A111DW04E8300003CC4EA5",
                  "invoiceStatus": "APPROVED",
                                                     -H 'Authorization: Bearer eyJhbGci...[ JWT Token ]...klQXOM-
                                                                                                                               invoice-status
                 "article6Status":
                                                   uA'
راهنما در صفحه ۴۴
                 "NOT EXCEEDED",
                   "error": null
```

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند «دستورالعل فني اتصال به سامانه مودمان »



۵ - دریافت چالش تصادفی و احراز هویت

مکانیزم احراز هویت در وبسرویس 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.

1-4 مراحل احراز هویت هر درخواست

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

- ۱. دریافت چالش تصادفی ٔ (رشتهی تصادفی)
- onnce و ساختن payload تو كن ronce و ساختن payload تو كن JWT.
- ۳. ایجاد header توکن JWT براساس ساختار مشخص و قراردادن گواهی امضا در آن
 - payload و payload براساس استاندارد JWS و ساخت توکن $^{
 m ext{ iny P}}$
 - فراخوانی درخواست بعدی با قرار دادن تو کن در سر آیند 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 می دهد. شما باید قبل از منقضی شدن این رشته آن را به همراه گواهی امضای خود امضا کرده و در در خواست بعدی در بخش Http Header به عنوان توکن ارسال نمائید.

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

Nonce *

شناسه سند RC_TICS.IS_v1.4

سند « دستورالعمل فنی اتصال به سامانه مودیان »



بهمن ۱۴۰۳

$\Delta - 1 - 1 - 0$ دریافت چالش تصادفی

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

Get Nonce – چالش تصادفی		
https://tp.tax.gov.ir/requestsmanager/api/v2/nonce	آدرس	
GET	Method	
• timeToLive: مدت زمان اعتبار رشته تصادفی به ثانیه		
○ نوع ورودی: اختیاری		
o محل قرار گیری: Request Params	ورودى	
o مقدار پیشفرض: ۳۰		
مقادیر مجاز: ۱۰ تا ۲۰۰		
• nonce: رشته تصادفی تولید شده		
• expDate: زمان انقضای رشته تصادفی	خروجي	

نمونه درخواست دريافت چالش تصادفي:

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

خروجي برابر است با:

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

امضای Nonce مضای $-Y-1-\Delta$

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

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

ىند « دستورالعمل فنى اتصال به سامانه موديان »



ساختار توكن JWS

یک شیء JSON دارای فیلدهای زیر:

- alg: الگوريتم امضا: RS256
- x5c: لیستی که شامل گواهی امضای مودی باشد. کد شده به فرمت Base64
 - sigT: زمان امضای تو کن

٥ فرمت:

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

نمونه:

2023-05-13T10:44:47Z

• sigT: لیستی از فیلدهای ضروری در قسمت Header. تنها شامل رشتهی "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 می توانید در انتهای آن عبارت "0330+" را اضافه کنید:

Header

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

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

یک شیء Json دارای دو فیلد زیر:

- nonce: رشته تصادفی یکبارمصرف دریافت شده
 - clientId: شناسه ارسال كننده صور تحساب

Payload

- برای مودیان همان شناسه حافظه صادر کننده صور تحساب
 - برای شرکتهای معتمد شناسه شرکت معتمد

ورودي الگوريتم امضا برابر است با:

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

Signature

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند «دستورالعل فنی اتصال به سامانه مودیان »



الگوریتم مورد استفاده در امضای توکن، RSASSA-PKCS1-v1_5 using SHA-256 میباشد.

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

مطابق استاندارد RFC7515 قالب چیدمان تو کن JWS به صورت زیر است:

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

توجه کنید که فرمت Header بستهی JWS و محتویات بسته (Payload) باید حتما utf-8 باشد و باید می Header برای امضا و تولید توکن به فرمت Base64URL کد می شود. برای اطلاعات https://www.rfc-editor.org/rfc/rfc7515 را مشاهده کنید: RFC7515 را مشاهده کنید:

لازم به ذکر است گواهی استفاده شده در فرآیند امضای توکن احراز هویت میبایست معتبر بوده و کد ملی/شناسه ملی موجود در گواهی 6 با مشخصات ارسال کننده در خواست (صاحب clientId) منطبق باشد.

بعنوان مثال فرض كنيد Header توكن ما يك Json به شكل زير باشد:

{"crit":["sigT"],"sigT":"2024-03-06T13:05:50Z", "x5c":["MIIDejCCAmKgAwIBAgIUV27QXqJjK2EgFy9zeYkpsX+ISPswDQYJK oZIhvcNAQELBQAwcTELMAkGA1UEBhMCSVIxDDAKBqNVBAqMA1RlaDEMMAoGA1UEBwwDVGVoMREw DwYDVQQKDAhNb2hheW1lbjEMMAoGA1UECwwDVGF4MSUwIwYJKoZIhvcNAQkBFhZtLm1hbHZlcmR pQG1vaGF5bWVuLmlyMB4XDTIzMDMyNDEzMjgyM1oXDTI0MDMyMzEzMjgyM1owTTEPMA0GA1UEAw wGQW56YWxpMRcwFQYDVQQKDA5RdW9WYWRpcyBHcm91cDELMAkGA1UEBhMCSVIxFDASBgNVBAUTC zE0MDAzNzc4OTkwMIIBIjANBqkqhkiG9w0BAQEFAAOCAQ8AMIIBCqKCAQEAzLqyk5KO6+j9d1ud 0ilJArrZ3Whw/w9wEzHB9yXwENRa5fm5AbRukMF5b6VGeKzD6LZuL9+tfdFfWyPcjI++qGNywzR mEHKpTnzP1t6NyuXKfm4nBVAblsugSw8Y5DEXRfTqILqBWN/pZ4zGlifEALMcGAs7ADcjnv7b/t M2wxr9rHxsCvW4HvlzQasK8Qr1CrKqT0EI66rSXCHep/uIONDWp0W2OelMlZtM6AAjWXRLGcshP IHuK+ZLfAFxWtoGonf6qN9ypos2B18D/EFa8WHON62eYKT0kW3jBVa3yPEkRwkdDjDu/3CPzymh f3WFYwxpb4t35oWb/qUXGVIdvwIDAQABoy4wLDAfBgNVHSMEGDAWgBSx+Oq+RO3x/FmyCp+jcmf OH+Fn9TAJBgNVHRMEAjAAMAOGCSqGSIb3DQEBCwUAA4IBAQAgKATXlnS+pPtAiRIYGtydVU5Vi7 Aq+D6QW07uFqcB7vBhddN3yX21VVcwpTNJzhv8UCM+mDMvlmsRVKVtMoo5fHfII92/Wo8rUz1RP +yhyCk0Vz8I11v+bjLwVur/agC/s5Rf0m66pNNjFZ9J3S2N3lChXYwz2vvA8pdAYvWTu9g5u4FM FqlsaLwMGC+WaA0g3KYzRkdWRy1vd23hLTUcVsWM8wpgZ11wEGE1khca/Sd0mCU2HG5vIbqFfTj A6to0fY07CE5fD8aR3UcXjNduosV052ZqCX5SabrhFS3AGHFRjpFnI5LZespiCXSA8Sv3kOSCSR QKqFbiwSFM8Zjg"], "alg": "RS256"}

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

^۵ فیلد SERIALNUMBER در قسمت SUBJECT گواهی امضاء

RC_TICS.IS_v1.4

سند « دستورالعمل فنی اتصال به سامانه مودیان »



بهمن ۱۴۰۳

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

با امضای رشته با الگوریتم RS256 و الصاق امضای تولید شده به رشته ی اصلی (به وسیله ی یک ".")، تو کن JWT ساخته می شود:

eyJjcml0IjpbInNpZ1QiXSwic2lnVCI6IjIwMjQtMDMtMDZUMTM6MDU6NTBaIiwieDVjIjpbIk1 JSURlakNDQW1LZ0F3SUJBZ01VVjI3UVhxSmpLMkVnRnk5emVZa3BzWCtJU1Bzd0RRWUpLb1pJaH ZjTkFRRUxCUUF3Y1RFTE1Ba0dBMVVFQmhNQ1NWSXhEREFLQmdOVkJBZ01BMVJsYURFTU1Bb0dBM VVFQnd3RFZHVm9NUkV3RHdZRFZRUUtEQWhOYjJoaGVXMWxiakVNTUFvR0ExVUVDd3dEVkdGNE1T VXdJd11KS29aSWh2Y05BUWtCRmhadExtMWhiSFpsY21ScFFHMXZhR0Y1Y1dWdUxtbHlNQjRYRFR Jek1ETX10REV6TWpneU0xb1hEVEkwTURNeU16RXpNamd5TTFvd1RURVBNQTBHQTFVRUF3d0dRVz U2WVd4cE1SY3dGUV1EV1FRS0RBNVJkVz1XWVdScGN5QkhjbTkxY0RFTE1Ba0dBMVVFQmhNQ1NWS XhGREFTQmdOVkJBVVRDekUwTURBek56YzRPVGt3TUlJQklqQU5CZ2txaGtpRz13MEJBUUVGQUFP Q0FROEFNSUlCQ2dLQ0FRRUF6TGd5azVLTzYraj1kMXVkMGlsSkFyclozV2h3L3c5d0V6SEI5eVh 3RU5SYTVmbTVBY1J1a01GNWI2VkdlS3pENkxadUw5K3RmZEZmV31QY2pJKytnR055d3pSbUVIS3 BUbnpQMXQ2Tn11WEtmbTRuQ1ZBYmxzdWdTdzhZNURFWFJmVHFJTGdCV04vcFo0ekdsaWZFQUxNY 0dBczdBRGNqbnY3Yi90TTJ3eHI5ckh4c0N2VzRIdmx6UWFzSzhRcjFDcktnVDBFSTY2c1NYQ0h1 cC91SU90RFdwMFcyT2VsTWxadE02QUFqV1hSTEdjc2hQSUh1SytaTGZBRnhXdG9Hb25mNnF00X1 wb3MyQjE4RC9FRmE4V0hPTjYyZV1LVDBrVzNqQ1ZhM31QRWtSd2tkRGpEdS8zQ1B6eW1oZjNXR1 13eHBiNHQzNW9XYi9xVVhHVklkdndJREFRQUJveTR3TERBZkJnT1ZIU01FR0RBV2dCU3grT3ErU k8zeC9GbX1DcCtqY21mT0qrRm45VEFKQmdOVkhSTUVBakFBTUEwR0NTcUdTSWIzRFFFQkN3VUFB NE1CQVFBZ0tBVFhsblMrcFB0QWlSSV1HdHlkV1U1Vmk3QXErRDZRVzA3dUZxY0I3dkJoZGROM31 YMmxWVmN3cFROSnpodjhVQ00rbURNdmxtc1JWS1Z0TW9vNWZIZklJOTIvV284clV6MVJQK3loeU NrMFZ60EkxMXYrYmpMd1Z1ci9hZ0MvczVSZjBtNjZwTk5qRlo5SjNTMk4zbENoWFl3ejJ2dkE4c GRBWXZXVHU5ZzV1NEZNRnFsc2FMd01HQytXYUEwZzNLWXpSa2RXUnkxdmQyM2hMVFVjVnNXTTh3 cGdaMTF3RUdFMWtoY2EvU2QwbUNVMkhHNXZJYnFGZlRqQTZ0bzBmWTA3Q0U1ZkQ4YVIzVWNYak5 kdW9zVk81MlpxQ1g1U2FicmhGUzNBR0hGUmpwRm5JNUxaZXNwaUNYU0E4U3Yza09TQ1NSUUtxRm Jpd1NGTThaamciXSwiYWxnIjoiUlMyNTYifQ.ew0KICAibm9uY2UiOiAiOTFkYzI4YWYtNGM5NS 00N2YwLTk5MTMt0Ddm0DE2MmIxNzA4LTE3MDk3MTc3NDk4NjIiLA0KICAiY2xpZW50SWQi0iAiQ TExMj12Iq0KfQ.qPsK S-76JrYRerFsb18SqVSNQTcUAd1o496mE 5XOfbw1BgLd3bC33Vxrfqs0lpxSm5hyiKpMYkaz-GPWXt9meoHozRNIFAGimWukE26pH7VJD4vJqfWN784k82XwHRLv1UVoPkzfmtRiFYTwI2hGc1B7 AfY I6cP5uGMBOY3Kqok0hhlfQyBM EIoSRNSW3JBAzHQea-EIm55oXkvXo 2lwsmGHXngFA6qhDbzuHJ2mkItor2HJjZTbND9sxN-X1ZqSuM7i6izvxxTuSaQMWAfTrEv9d2BzG1ZT1zcFBZVXLAza13Bh74P5DhWsoOR8q0EJvgMvbK

تکه کد زیر به زبان جاوا عملیات ساخت تو کن از روی Nonce را انجام می دهد. لازم به ذکر است تمامی این فرآیندها در کیت توسعه نرمافزاری جاوا و .net پیاده سازی شده اند و این تکه کد صرفا جهت آشنایی بهتر با فرآیند تولید تو کن 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();
```

RC_TICS.IS_v1.4

سند « دستورالعمل فنی اتصال به سامانه مودیان »



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 = {\text{"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 می شود. سپس گواهی امضای مودی در قالب یک شیء از نوع X509Certificate باز می شود. سپس تاریخ امضا به فرمت مشخص شده تولید می شود. در نهایت با ساخت header در خواست و قرادادن آن در کنار payload داده شده و با در اختیار قرار داشتن کلید خصوصی امضا، تو کن jwt ساخته می شود. جهت امضای رشته و تولید jwt در این تکه کد از کتابخانه ی jose-4j نسخه ی ۹.۳۰ استفاده شده است. همچنین تکه کد زیر به زبان T.۳۰ همین عملیات را انجام می دهد:

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

RC TICS.IS v1.4

سند « دستورالعمل فنی اتصال به سامانه مودیان »



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 = "{\mbox{"nonce}":\mbox{"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 RC_TICS.IS_v1.4

سند « دستورالعمل فنی اتصال به سامانه مودیان »



بهمن ۱۴۰۳

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

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

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

بررسی امضای توکن JWS بدین صورت است که هر یک از شرایط زیر برای صحت امضای بسته بررسی می شوند و در صورت و جود خطا در هر بخش صحت امضای بسته زیر سوال می رود و توکن فرستاده شده مورد قبول واقع نمی شود:

- ا. ساختار كلى بستهى payload ،header) JWS و signature) ارسال شده صحيح باشد.
- ۲. امضای موجود در بسته ی JWS با گواهی امضای فرستاده شده در قسمت header تو کن ارسالی Verify شود.

Header 9

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند «دستورالعل فنی اتصال به سامانه مودیان »



- ۳. گواهی امضای فرستاده شده در header توسط یکی از مراکز میانی مورد اعتماد زیرسامانه ی Trusted جمع آوری صادر شده باشد و امضای گواهی با یکی از گواهی های موجود در مخزن Verify شود.
 - ۴. تاریخ انقضای گواهی امضا سپری نشده باشد.
- $^{\Delta}$. در صورت وجود فیلد CRL Distribution Point در فیلدهای موجود در گواهی (قسمت (Extension) استعلام لیست گواهی های ابطال شده پیش از موعد از مرکز میانی مورد نظر گرفته می شود و بررسی می شود گواهی مورد نظر جزو گواهی های ابطال شده ی پیش از موعد نباشد.
- ⁹. در صورت وجود فیلد Authority Information Access در فیلدهای موجود در گواهی (قسمت OCSP) و وجود Method برابر با Access Method و وجود در گواهی گواهی که آدرس سرور OCSP مرکزمیانی صادر کننده ی گواهی می باشد، وضعیت گواهی استعلام گرفته می شود که گواهی دچار ابطال پیش از موعد نشده باشد.

6 - دريافت اطلاعات سرور

این وبسرویس اطلاعات سرور مانند timestamp و کلیدهای عمومی رمزگذاری سامانه مودیان را برمی گرداند. 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. نحوه ی کار این API به صورت زیر است:

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

RC TICS.IS v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



```
key o: کلید کد شده به فرمت Base64
```

- o id: شناسه کلید
- "RSA" فعلا برابر با algorithm 🔘
 - o purpose: مقدار ثابت ۱

نمونه درخواست ارسالي و پاسخ آن:

```
curl -X 'GET' \
  'https://tp.tax.gov.ir/requestsmanager/api/v2/server-information' \
  -H 'accept: */*' \
  -H 'Authorization: Bearer eyJhbGciOi...[JWT]...Jvl8fvHmOPKVA'
```

در صورت صحت توكن و درست بودن ساختار درخواست خروجي برابر است با:

۷ - ارسال صورتحساب

فرآیند ارسال صورتحساب هم مانند همهی فرآیندها در وبسرویس جمع آوری نیاز به احراز هویت فراخوانی کننده دارد. بنابراین از تکرار این مرحله صرفنظر می کنیم. فرض می کنیم عملیات گرفتن nonce امضای آن و ساخت تو کن 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

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

ىند « دستورالعمل فنى اتصال به سامانه موديان »



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 منحصربه فرد مالیاتی، صورتحساب را به شکل یکتا مشخص نمائیم. سپس باید صورتحساب را امضا کنیم و بستهی JWS تولید نمائیم. در مرحلهی بعدی باید از صورتحساب امضا شده، به وسیله کلید عمومی سازمان (که از طریق GET server-information دریافت می گردد) بستهی رمزشده JWE ساخته شود و سپس برای وبسرویس جمع آوری ارسال شود.

٧- ١- جزئيات فرآيند ارسال صورتحساب

TaxId تولید شمارهی منحصربه فرد مالیاتی -1-1-7

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

٧- ١- ٢- امضاي صورتحساب

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

TWE - A - The add and	
امضای صور تحساب - JWS	
یک شیء JSON دارای فیلدهای زیر:	
• alg: الگوريتم امضا: RS256	
• x5c: لیستی که شامل گواهی امضای مودی باشد. کد شده به فرمت Base64	Header
• sigT: زمان امضای توکن	
Format: yyyy-MM-dd'T'HH:mm:ss'Z' Example: 2023-05-13T10:44:47Z	

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



• crit: لیستی از فیلدهای ضروری در قسمت Header. تنها شامل رشتهی "sigT" •	
ء JSON صورتحساب	Payload شی
دى الگوريتم امضا:	ورو
ASCII(BASE64URL(UTF8(JWS Protected Header)) '.' BASE64URL(JWS Payload))	Signatura
وريتم: RSASSA-PKCS1-v1_5 using SHA-256	Signature
د خصوصی: کلید خصوصی متناظر با گواهی فرستاده شده در بخش Header	كليا

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

به عنوان نمونه فرض كنيد Json صورتحساب ما بعد از توليد شماره مالياتي به شكل زير است:

```
{"header":{"taxid":"All21604C220002F095011","inno":"49321217","indatim":168 3997837988,"inty":1,"inp":1,"ins":1,"tins":"14003778990","tob":2,"bid":"101 00302746","tinb":"10100302746","tprdis":20000,"tdis":500,"tadis":19500,"tva m":1755,"todam":0,"tbill":21255,"setm":2},"body":[{"sstid":"2710000138624","sstt":"كارى فولاد صنعت قطعات سرسيلندر","mu":"164","am":2,"fee":10000,"prdis":20000,"dis":500,"adis":19500,"v ra":9,"vam":1755,"tsstam":21255}],"payments":[]}
```

حال یک شیء JWS میسازیم که Header آن مقدار زیر باشد:

{"crit":["sigT"],"sigT":"2024-03-06T13:16:11Z", "x5c": ["MIIE7DCCA9SgAwIBAgISAM4ybFjIYlezw/6Ly2CQYYNBMA0GCSqGS Ib3DQEBCwUAMIG7MQswCQYDVQQGEwJJUjEZMBcGA1UECgwQTm9uLUdvdmVybm1lbnRhbDEkMCIG A1UECwwbQW1uYWZ6YXIgR29zdGFyLWUgU2hhcmlmIENvMTQwMgYDVQQLDCtQYXJzU21nbiBJbnR lcm1lZGlhdGUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5MTUwMwYDVQQDDCxQYXJzU2lnbiBQcml2YX RliEludGVybWVkaWF0ZSBTaWx2ZXIgQ0EgLSBHMzAeFw0yMzEwMTgwNjQyMTZaFw0yNDEwMTIwN jQyMTZaMIGyMSAwHgYDVQQDDBdBbGkgU2hpcm1vaGFtYWRpIFtTaWduXTELMAkGA1UEBhMCSVIx DzANBgNVBCoMBti52YTbjDETMBEGA1UEBwwK2KrZh9ix2KfZhjEVMBMGA1UECgwMVW5hZmZpbGl hdGVkMRMwEQYDVQQFEwowMDIzNDU3NzA4MRMwEQYDVQQIDArYqtmH2LHYp9mGMRowGAYDVQQEDB HYtNuM2LEg2YXYrdmF2K/bjDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAIm7YPJLA bIyHftOB9SsMps1OeFMJ5+bRZLa4dE5cf404Qb2K6m+ITxT8sD009mDLqbfxTCq1+ehlbAl/yug XdF5+rGYQYX/yaJf+vkaAq162vqdRvbVvkhNr1XI2rI+sXfGJBcGnceskoVf7rm+RTciOmAA3Zh cjdU3jFmU1/Am8VBJ83kK8Qf8I6ZtFZhHL1Yp051xLVs5QI4/lwmKxkEkmG+VgGV22Mkve3Yw1P oeMyc00110BvFd3iiEnAUtHuIKF6cFwWia0hIJLvd+s/W7LuVQMNVYeu+J64zDqYBwDaSt4L+eo fT6ksg6aslQSZdf/7VGyDGIqcjTet1E/C8CAwEAAaOB8DCB7TAdBgNVHQ4EFgQUepvjaOKnzm8N 4C/+g1F4neodzaMwHwYDVR0jBBgwFoAUFMcOIHyJ0RZ/yrlp6IfJLEaC+lUwNAYDVR0fBC0wKzA poCegJYYjaHR0cDovL2wyLnBhcnNzaWduY2EuaXIvUFNfTDJDQS5jcmwwDgYDVR0PAQH/BAQDAg bAMBYGA1UdJQEB/wQMMAoGCCsGAQUFBwMCMDcGCCsGAQUFBwEBBCswKTAnBqqrBqEFBQcwAYYba HROcDovL2wyLnBhcnNzaWduY2EuaXI6ODEvMBQGA1UdIAQNMAswCQYHYIJsZQEBAjANBgkqhkiG 9w0BAQsFAAOCAQEAcw2hdV1YN8xHXsQq4X6YWtgyUsK92CTILb/j2jYfIGXlwLCYxR6zPFuoqmj VG9Txs3NEPQirsVwqoIUzljTZnBU/WlPjeqPyWadQooRvg/64Ahd88A8YJf3Yvv1Dax8rUANX+A Qd0930xAr7hfCISTHFmhhw5GoJ153vh0idhekeK6//iwvLugPA9k0Qu0W0bWsJ2Ctj2zWhCXMdz

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



IajqkpEmyBJxe4yj9ZGyezjSmPb+khDgvEsbrOPcWy3WTsx80S3Shph18ywNQTRd6OximDXs14+
1L0BlZav6o0DpTlkF40OmoPkoZwQkJNxBrNrKWDeK39vRR56yPP4p+04Ww=="],"alg":"RS256
"}

و سپس آن را با استفاده از کلید خصوصی که در اختیار داریم امضا می کنیم. حال صورتحساب امضا شده به صورت یک JWS در می آید:

eyJjcml0IjpbInNpZ1QiXSwic2lnVCI6IjIwMjQtMDMtMDZUMTM6MTY6MTFaIiwieDVjIjpbIk1 JSUU3RENDQT1TZ0F3SUJBZ01TQU00eWJGak1ZbGV6dy82THkyQ1FZWU5CTUEwR0NTcUdTSW1zRF FFQkN3VUFNSUc3TVFzd0NRWURWUVFHRXdKS1VqRVpNQmNHQTFVRUNnd1FUbTl1TFVkdmRtVnlib TFsYm5SaGJERWtNQ01HQTFVRUN3d2JRVzF1WVdaNllYSWdSMj16ZEdGeUxXVWdVMmhoY21sbU1F TnZNVFF3TWdZRFZRUUxEQ3RRWVhKelUybG5iaUJKYm5SbGNtMWxaR2xoZEdVZ1EyVnlkR2xtYVd OaGRHVWdRWFYwYUc5eWFYUjVNVFV3TXdZRFZRUUREQ3hRWVhKelUybG5iaUJRY21sMllYUmxJRW x1ZEdWeWJXVmthV0YwWlNCVGFXeDJaWElnUTBFZ0xTQkhNekFlRncweU16RXdNVGd3TmpReU1UW mFGdzB5TkRFd01USXdOa1F5TVRaYU1JR31NU0F3SGdZRFZRUUREQmRCYkdrZ1UyaHBjbTF2YUdG dflXUnBJRnRUYVdkdVhURUxNQWtHQTFVRUJoTUNTVkl4RHpBTkJnTlZCQ29NQnRpNTJZVGJqREV UTUJFR0ExVUVCd3dLMktyWmg5aXgyS2ZaaGpFVk1CTUdBMVVFQ2d3TVZXNWhabVpwYkdsaGRHVm tNUk13RVFZRFZRUUZFd293TURJek5EVTNOekE0TVJNd0VRWURWUVFJREFyWXF0bUgyTEhZcD1tR 01Sb3dHQV1EV1FRRURCSF10TnVNMkxFZzJZWF1yZG1GMksvYmpEQ0NBU013RFFZSktvWklodmNO QVFFQkJRQURnZ0VQQURDQ0FRb0NnZ0VCQUltN11QSkxBYkl5SGZ0T0I5U3NNcHMxT2VGTUo1K2J SWkxhNGRFNWNmNDA0UWIySzZtK01UeFQ4c0RPMDltRExxYmZ4VENxMStlaGxiQWwveXVnWGRGNS tyR11RWVqveWFKZit2a2FBcTE2MnZxZFJ2Y1Z2a2hOcjFYSTJySStzWGZHSkJjR25jZXNrb1ZmN 3JtK1JUY21PbUFBM1poY2pkVTNgRm1VMS9BbThWOko4M2tLOFFmOEk2WnRGWmhITDFZcDA1MXhM VnM1UUk0L2x3bUt4a0VrbUcrVmdHVjIvTWt2ZTNZdzF0b2VNeWMwTzExMEJ2RmOzaWlFbkFVdEh 1SUtGNmNGd1dpYTBoSUpMdmQrcy9XN0x1V1FNT1ZZZXUrSjY0ekRxWUJ3RGFTdDRMK2VvZ1Q2a3 NnNmFzbFFTWmRmLzdWR31ER01xY2pUZXQxRS9DOENBd0VBQWFPQjhEQ0I3VEFkQmdOVkhRNEVGZ 1FVZXB2amFPS256bThONEMvK2cxRjRuZW9kemFNd0h3WURWUjBqQkJnd0ZvQVVGTWNPSUh5SjBS Wi95cmxwNklmSkxFYUMrbFV3TkFZRFZSMGZCQzB3S3pBcG9DZWdKWVlqYUhSMGNEb3ZMMnd5TG5 CaGNuTnphV2R1WTJFdWFYSXZVRk5mVERKRFFTNWpjbXd3RGdZRFZSMFBBUUqvQkFRREFnYkFNQ1 1HQTFVZEpRRUIvd1FNTUFvR0NDc0dBUVVGQndNQ01EY0dDQ3NHQVFVRkJ3RUJCQ3N3S1RBbkJnZ 3JCZ0VGQ1Fjd0FZWWJhSFIwY0Rvdkwyd31MbkJoY250emFXZHVZMkV1YVhJNk9ERXZNQ1FHQTFV ZTjh4SFhzUXE0WDZZV3RneVVzSzkyQ1RJTGIvajJqWWZJR1hsd0xDWXhSNnpQRnVvcW1qVkc5VH hzM05FUFFpcnNWd3FvSVV6bGpUWm5CVS9XbFBqZXFQeVdhZFFvb1J2Zy82NEFoZDg4QThZSmYzW XZ2MURheDhyVUFOWCtBUWQwOTNPeEFyN2hmQ01TVEhGbWhodzVHb0oxNTN2aDBpZGhla2VLNi8v aXd2THVnUEE5azBRdTBXT2JXc0oyQ3RqMnpXaENYTWR6SWFqcWtwRW15Qkp4ZTR5ajlaR3llemp TbVBiK2toRGd2RXNick9QY1d5M1dUc3g4MFMzU2hwaGw4eXdOUVRSZDZPeGltRFhzMTQrbEwwQm xaYXY2bzBEcFRsa0Y0ME9tb1Brb1p3UWtKTnhCck5yS1dEZUsz0XZSUjU2eVBQNHArMDRXdz09I 10sImFsZyI6IlJTMjU2In0.eyJoZWFkZXIiOnsidGF4aWQiOiJBMTEyMTYwNEMyMjAwMDJGMDk1 MDExIiwiaW5uby16IjQ5MzIxMjE3IiwiaW5kYXRpbSI6MTY4Mzk5NzgzNzk4OCwiaW50eSI6MSw iaW5wIjoxLCJpbnMiOjEsInRpbnMiOiIxNDAwMzc3ODk5MCIsInRvYiI6MiwiYmlkIjoiMTAxMD AzMDI3NDYiLCJ0aW5iIjoiMTAxMDAzMDI3NDYiLCJ0cHJkaXMi0jIwMDAwLCJ0ZGlzIjo1MDAsI nRhZGlzIjoxOTUwMCwidHZhbSI6MTc1NSwidG9kYW0i0jAsInRiaWxsIjoyMTI1NSwic2V0bSI6 Mn0sImJvZHkiOlt7InNzdGlkIjoiMjcxMDAwMDEzODYyNCIsInNzdHQiOiLYs9ix2LPbjNmE2Yb Yr9ixINmC2LfYudin2Kog2LXZhti52Kog2YHZiNmE2KfYryDYs9in2LLbjCIsIm11IjoiMTY0Ii wiYW0iOjIsImZlZSI6MTAwMDAsInByZGlzIjoyMDAwMCwiZGlzIjo1MDAsImFkaXMiOjE5NTAwL CJ2cmEiOjksInZhbSI6MTc1NSwidHNzdGFtIjoyMTI1NX1dLCJwYXltZW50cyI6W119.AVPw0w2 IG7BJ5zqlQYrP vvBT1wX0eB4ZP77vvQkTN2At-zb8hpFeqG-

uqui99cvR4i27GVnKcMpLBNVmMrL4FODTXqKn053bJ8oPJhbnUFhIkOAcoRmPUOtmO5jsWvocAL07Bh-m8B7nQG7d-

 $\label{local_model} RLEXViwbaCmMI7hzMCBzMm3P0Sr2cBVDrK8FUR_8VHb219gUm52A4Wy8i4moHc1Gi_65O3vrNX9bN3DiJSS_me5W0isE0GjglB3zHTMzE6MAZMpBbVJYfJOK-h-\\$

RKJaWLAlIvZYbYmhVMbfuxFB5Q9DlqDsvc0ie4Nn3Qs0sMVPcNO335ANSMu7wgFPqYmEK5aEw

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

ىند «دستورالعل فنى اتصال به سامانه موديان »



توجه کنید که بررسی اعتبار امضا و گواهی امضا کننده ی صورتحساب نیز عینا همانند بررسی توکن JWS میباشد و در کنار بررسی گواهی امضای صادر کننده ی صورتحساب و تاریخ انقضای گواهی، از سرور OCSP و CRL صادر کننده ی گواهی استعلامات لازم برای اطمینان نسبت به اعتبار و صحت گواهی گرفته می شود.

لازم به ذکر است گواهی استفاده شده در فرآیند امضای صورتحساب میبایست معتبر بوده و کد ملی/شناسه ملی موجود در گواهی دسترسی ارسال صورتحساب برای شناسه یکتای حافظه مالیاتی مربوطه را داشته باشد.

V - V - V رمزگذاری صورتحساب

در مرحله ی بعد باید صورتحساب امضاشده را رمزگذاری کنیم. این کار باعث می شود هیچ شخص دیگری به جز سرور سامانه ی مودیان توانایی باز کردن و مشاهده محتویات صورتحساب را نداشته باشد. الگوریتم دیگری به جز سرور سامانه ی مودیان توانایی باز کردن و مشاهده محتویات صورتحساب را نداشته باشد. الگوریتم AES AES (AES/GCM/NoPadding) AES256-GCM می باشد و کلید RSAES OAEP using SHA-256 and MGF1 with) RSA-OAEP-256 می نیز از طریق الگوریتم می شود که این فرآیند بر اساس استاندارد JWE انجام می شود. الگوریتم رمزگذاری AES 256-GCM دارای ۴ ورودی و ۲ خروجی است. ورودی های الگوریتم عبارتند از محتوای بسته یا همان (Additional Authentication Data) AAD دارای ۴ و داده اضافی احراز هویت (Authentication tag). ابتدا یک کلید خروجی های الگوریتم عبارتند از بسته ی رمزشده و تک احراز هویت (Initial Vector). ابتدا یک کلید AAD به همراه ۹۶ بیت ۱۷ (یا همان Vector) تولید می شود. داده اولیه AAD هم از روی عنوان ورودی به الگوریتم داده می شود تا داده رمز شده و Payload (رشته ی SWB صور تحساب امضا شده) به عنوان ورودی به الگوریتم داده می شود تا داده رمز شده و Payload رمز شده می توان با الگوریتم Authentication تا کلید عمومی سازمان، ۱۷ و تک شناسایی، یک بسته Authentication در کنار کلید آن را برای و ب سرویس سامانه ی مودیان ارسال نمود.

^۷ فیلد SERIALNUMBER در قسمت SUBJECT گواهی امضاء

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



ساختار شيء JWE:

بستهی رمز شده – JWE	
یک شیء Json دارای فیلدهای زیر:	
• alg: مقدار "RSA-OAEP-256" مقدار	
• enc: مقدار "A256GCM" مقدار	Header
• kid: شناسه کلید عمومی رمزگذاری سامانه مودیان	سرآيند
نمونه:	
{"alg": "RSA-OAEP-256", "enc": "A256GCM", "kid": "6a2bcd88-a871-4245-a393-2843eafe6e02"}	
کلید متقارن رمزگذاری AES به طول ۳۲ بایت (۲۵۶ بیت) را با استفاده از الگوریتم	II41
RSAES OAEP using SHA-256 and MGF1 with) RSA-OAEP-256	Encrypted Symmetric
SHA-256) با کلید عمومی رمزگذاری سامانه مودیان به طول ۴۰۹۶ بیت، رمز	Key
می کنیم. کلید رمز شده ۵۱۲ بایت طول دارد که Base64URL Encoded آن را در	کلید متقارن رمز شده
این قسمت قرار میدهیم.	5500
Encode شدهی ۱۲ بایت (۹۶ بیت) iv به فرمت Base64URL که رشتهای به طول	
۱۶ کاراکتر می شود.	Initial Vector
رشتهی JWS صورتحساب امضا شده که با استفاده از کلید متقارن و با الگوریتم	Payload
AES256-GCM رمز می شود.	محتوای رمز
	شده Authentication
تگی که به منظور اطمینان از دستکاری نشدن محتوای پیام رمز شده و کلیدها استفاده	Tag
می شو د.	تک 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)) | '.' | BASE64URL(JWE Encrypted Key) | '.' | BASE64URL(JWE Initialization Vector) | '.' | BASE64URL(JWE Ciphertext) | '.' | BASE64URL(JWE Authentication Tag)
```

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند «دستورالعل فنی اتصال به سامانه مودبان »



مراحل رمز گذاری صور تحساب:

سر آیند JWE به فرمت utf-8 برابر است با:

{"alg":"RSA-OAEP-256","enc":"A256GCM","kid":"6a2bcd88-a871-4245-a3932843eafe6e02"}

که Encode شده آن به فرمت Base64URL می شود:

eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIiwia2lkIjoiNmEyYmNkODgtYTg 3MS00MjQ1LWEzOTMtMjg0M2VhZmU2ZTAyIn0

توجه کنید که رشتهی 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 رمزگذاری 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+Wm11hzjjhAGfSUOuDvOKRoUEQwP8oUcXRmYzcvCUgcfoRT5iz7HbovqH+bIeJwT4rmLmF cbfPke+E3DLUxOtIZifEXrKXWgSVPkRnhMgym6UiAtnzwA1rmKstJoWpk9Nv34CYgTk8DKQN5jQ Jqb9L/Ng0zOEEtI3zA424tsd9zv/kP4/SaSnbbnj0evqsZ29X6aBypvnTnwH9t3gbWM4I9eAVQh PYClawHTqvdaz/O/feqfm06QBFnCgL+CBdjLs30xQSLsPICjnlV1jMzoTZnAabWP6FRzzj6C2sx w9a/WwlXrKn3gldZ7Ctv6Jso72cEeCeUI1tzHMDJPU3Qy12RQzaXujpMhCz1DVa47RvqiumpTNy K9HfFIdhgoupFkxT14XLD165S55MF6HuQvo/RHSbBJ93FQ+2/x/Q2MNGB3BXOjNwM2pj3ojbDv3 pj9CHzvaYQUYM1yOcFmIJqJ72uvVf9Jx9iTObaNNF6pl52ADmh85GTAH1hz+4pR/E9IAXUI1/Yi UneYu0G4tiDY4ZXykYNknNfhSgxmn/gPHT+7kL31nyxgjiEEhK0B0vagWvdRCNJSNGWpLtlq4F1 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 ۲۵۶-RSA با ورودهای یکسان، متقاوت خواهد بود:

lRs_vcZlauJs4VwED3wZGr3wJDbg8It9zBStuJgqf7TiGs3kUCSulPwA6jRA-8xuHTpNtKr1w0hsNbUhsx-

 $3BL5zGaDzsSekA1AZVevVy2qOrfId60xLOb81SpVnSRR_K3jRHDWfH_ZDgZqMoM2mv6qFvb8GgGFV59_jIkhctX73Y6iqe3NCask2CT0Ine3SUFVxt_OBqnBCwgDLrauGyisQbpVN1JJRjsWPeyXA0OWvlECnRSLS93-prnMrfLTU_JHUyU304-cq7gVu7OATP1NB78L8m0-$

MiIF tr0mpbaEneOLDbimNYt2UVgn1thJsvh5Na30GKY5t-ISHoWhX-

DvVHp3KTEpp0bkC8IczZt-jg-

2vdYhyM7Sz1H0c9w2EvSSryYsAVonOojl4yWeaNhP_7mk09hgu1MUkr91Tfr-

U1k3zFHyCClfJzHj3t3uebS2mFDEyuao7K4omC335_VYsCi6kRSU421AW1_8V21RxaS2VDBQbgoCgr3UQQxsoSRIG3v1-OBgTgZ9slEGZnEihaptab-

7IegnXIbhZNA8Onzy0wKW2S6r8M2eDd010hGaDPGXcdWtOpC-O-

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



cvu9MJTp4MRDx5dYe2rRQaI_A7WS5vJGkjwdRRpfhaJhGoXA7Wc6eUmB_UFOvPfsGQdFXPBUB3vh6jPfsER6hnXjU

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

75ZoCOOVRqIWRyAs

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

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

Base64URL(Header):eyJhbGciOiJSU0EtT0FFUC0yNTYiLCJlbmMiOiJBMjU2R0NNIiwia2lkI
joiNmEyYmNkODgtYTg3MS00MjQ1LWEzOTMtMjg0M2VhZmU2ZTAyIn0

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-

141X0520tRcvrhp8D9cHCfYLTIonEo3MXYQ46Z8QTPv2ueCdiKztQDngTuczGGY3lve1cz-

tHqeAJZ92UG9cjouMVE7IY29ML7OrzPy66GJsVb3BZnmIm6vDNEMf9AL8LH3y-

H4rk9JmZjQbrRIU2AbmTGwRK0 FnQD660b-4nEMKfc51h9bk-

 $\label{local_constraint} $$dc8as3_0xFH2b0KxaiZDki8pDLumCFPQ9U9pfU7KUmkFl09FGF3FpryGX5DzEE_YprotK6lcEr9f8U5ooHS_PF06pprnL_CkXtimdJEnJgghk-$

 $5 \texttt{XdZ} \texttt{fdIM1R4ghYPDT_rfE0GjmroEaWOaoM3qXwDhdUFs1nb_48KAUOQY1ebgd9Ngi_ed-model} \\$

rh517TAj1wPCmgnPEY9SYIPeorurSwlMPPpI9NN-bjjBUhW1a4RxkCt5UeHDS--

bvRkPqD5DaiOQg2RD7n8cm6pzHKcKO16WpXSSFhIjK1-

l kevoprXPIEHtWik3PBSXYWDzl5Gc ET-aw2CF6xgWkUi-

vw512 ySvs66qrxGqubBQkOOxLLyUEmcxedPSCSs6q4eNqf-

SES0yZ9NR4uBs3WBsqs2h0Ftrn5ZKniMDQKtoU0LJvscjXBso6ckAVuvjBilY4zKgr07FjJ9zn-9xkStotxms0czBo-

 $fOsVunTuKypLBvTiwV4uykqUnsxbyOtuUvr10kLK1dma4F9q1gixRqfoMyn1o7seRDTRrTkBh_DkrF-$

AzNhZG3o1TC5bHUtwN5crc2dw3FkS4UMe1unQkusFL44MRqY3qbn_iP4NY8X3bWTWtp31kiFxKt ATTiZG_lvi5om1QwcA7a_mYQw47EjjvGTiSJQsfDM8d2WBlVDOV65xgcqy7OQVRPxfTo6jJu-X1MGd-RN2Lb_crLsnJGJ6kpdhqyF7ts_3gbWvryzKLJyDe2HM3izN6Kw0U4Ba-__YOMPV-mJECsVC5KUw9jRYhw6tdYSU41LXKRDnMyh-

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



cjRyuv4V347DOR280aGWsbqpqaDp4mdtkaABARhtO5BhbzzeSnHnEjTVZmdn8H5WifzGvqHCiGAz752CNNO000wCbpVoW2Jcq78XndubsxsXzkcq0XvsDxnKzdBdRkoYyTEd5tMOdxUZw_tpbXNQZFFwAB4ph_FtoYC0j50kGhEola6h7jguoFJu0CewloGSkvvqu2Ht4G9IfDkFs0tMTvdjHJJGWpDj9nQ_Mzn0QkKBPhGLM50yUtosIVd1FvrHCJuhkt3qsAP6OTHvgDswELnLMcOsoRB2qdVp6YSAOT3ZuRc6Bawwd5S78wd_o4ISW9pNMxNbHPueiXI_N48S9Zcb2ktwH6dB3rbkRwgXCEWcPheX8s5ik325PbY5RAs29fj45yISSZ-

6xlg9BwBXjg81TkNg18_6j0aI8ZZmDjL1EyjK0ojb9UpQUfjreakNAGhxSa5S_ethmI63Bs6_En XyzOKDP5sPmlyBgJ6RjXRSmVI8zqA1ETazPY93PYql_PqADQm48_Ocs1h_djjNNBHeA8ucYelX1 T8tcD-ENwrvJw8 2u1A1DWX-

FucPGQQLZc4PkwO4OCUeBlxDUsJFzedhX0cKEQr_b9zxhVT3C09yr3q6FyhqrYF892Kql06PmXBVEZrb-Q0piVZyozeordNJGRE016r8Al0hnc-KgUlkdZrxee_zzk9aV08CUO1-

fvBRCGOR12v EAcY17pnyfnCKmZH3u3Iq5D7-

T3JHJSZz2NuUFrCok81L87X0YbRCscW164VAEsF1QolakktKt8cNRQwj_95rtt1Ka06Fdg6Q-VK9NskncKRKnlWcIQT6Ec6eTmr1Ng7JaQ7dqkEh zThM8ifE-

Ak6jVdpMiHZ4NvdlOndCPbi1r7zFNrUeRI0BK5PWfOJA90YAnMJ3B7DkrAMyLhZMkKXp4UjEZSQhBhe lnD9VxL3rZcmRqEctFVmsTnyRZY-

pZ1Sx8gS__99WXrtNqD11R3njeHWJsCi35GoJJwWh3BFCJvsyeQcmsIkkN4RdBrwj_B-ZpUKJn1gvho2E7PPkvuMpMPSWr1c1zptCpzamAY2pTjBgmQ5NWDnxN87fUZN9YaJYMcqD7kb-kooJuNWw7TcF-YPo 31UHHWd3mKzBVFUeYEqqJBA-

9KroMQzfC7hc5QQkaA_oGVn0_8_AexX7fNDdXc6yRzM_msfGsbO6pMYegbEijS5F3DaopvpAmwdBbFlDRUIGSKpfODn9DNGB2BoqNn1mNPCuBsqGuPvF3RzgxP-1MoCI3Xf7RxG1DYr-

bTPsV6pyzinV5HaGSNRorYkXchaXhl19k4d9pfu_4uXeASFVG6WxzdpVwb_w769VQdVYL7KG0u4uC_MhWDH0w1DVEFySffBNPpZ6Z_lLYkbc8epocBH9HjJVFByP4gqVieVuDlX_tkK6QUwSPZTl36Be4uVf9luAJXZfn3IkMbj8KuRfLjwBE3N4MnjXbz4RHN5dZwaSJftRgYo_DaJPiqcGz1H3dB5B4i0A7bLA4H1TEIKLPom-

A1GnpRruGdoF7dD3dhx8HOKUt7ny7zMrYQWI86bmRzubnMZmi87GguvCoCP7o7ATMJIGprSDmg-3TJ5FGyeXaNRZO1EP1Dhc6uh19Pm_PYP718tKg5Z_dGgnFWwJp2SDweU7kvWgEUePJVa-HKd7iiRGP-

2cttS8ak4zlq_OjKkFRHi6A2uZ95Yg0dkWgBbHgCHbbuM5oBmIztFixmnHeoTrV3HPbBPw2jEX_XINhFVcYnfc1efs0Gh-

jKA4wrCgStq5bXRhMC5degaoQ0Sb5eY_S_Ehpz1yoA_JYDHp6t8FfnSMTNbM9LfoBTgZDdlrRmwd2dBVJxzkbhTpXo4dpShFRsL1vs0GV3wdELBuzMb3UaTyu-

rJy_DoblfPE8pmlC1NS2_WHrVXB0gJf91MaaIup_Fx7tJzSbqiNG9mFj6SQvMk0HvAyI195NpyFNX33x5NLFnF6125mZdn6MY6nLPeNu9P1yEadZ8uXnMtwfrAOuN83yS2XZDWKHPYSJOaVcsGAjRrcGLpulp-dcx1g0XVQgNR0KzaH7J3zbRJ-Lqf7V6w9aYT1JnHk21bof2oGp9NaWN1-Tq1OEvrAk3-

EqzyCigOG5A2YZdoRR_1rlCxfNCXz0dtRwM07IX_kEEEKHTs4lk970YTSa_SdhYNMUN0QPBLkjTts_YMnx8Y2wFumFy9Ji3K5o2GHB5nc0a1DioSi9gNEpFjv6pT_Tk9NDIFUBAwv8oV_qp41qFqSpA9g6G51madn0K6sonvAsRlDWNjxSBropg1stgWWCRe3Ucp_b9PhZht1rSuJsZynEqLCf9ZLn2lxfugLbIOdvaNZxkI2NtNHCv_CsiMFo76rC5SwCJ5uTtD64z53s2txbOPmhWpIGE63OKi3fQSZz5HZdBbidIRcM3vCEseMNw1A27F7BCIN6o9tZd-lX0Zkvh08Wts2d-c1Fs-

x5ssLWeoMPpGvnFjZ9pQBD8EyK34JsA5qPTVjLOD62ZRph8PdkiJIoE0es4QMyleVbUe9rbscIN F2m5YSHiRWWM5MFSpDFmT67EtriseeWQnVNQTU31_chDRut92yv2G3seSa8HHMLW0Gmq7W7hUUG uxLbUSVv74U7 55vpQM0fuRhJ7khTbZioN-

wBp32Zyy_phgMi5sOqV351PoCzpZ7ueQwbsS6kvABCj2PjoeQL2trqrjcfkPfLPUKsETgkVrgvijt55bzKmUG624fv1zJbgSt7t3rrPiVQyKflW0YJcx-

39sKDICQeEFpQp_7gnf7LoKKVPAISDLSSCHJro6R5Vm74INsQQjGn-

fH55R2sS4GVw74DfWF1k7wp9Upw3JjlgQ9MhRpVjUd98CprL-

jjdn4k4CuHxZPXEoXEfkvC8PO4HmDN1Od-

3ShVrilhJ1gLFpuM1814OylUju9bhHEM8R28YL7ftgWvtzhMkdw3BPM05Uzo29xAsS GZeDikFl

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعل فنی اتصال به سامانه مودیان »



db2E7CoZu3evhnrMsk9KWGbbrxcAZDFR1zhNJHJBFVPpjpxgoXy6Br3LAtZBnu217Zt5mfAF08h EG0baz-MS0hPahcfoE3S7c5xPcV4wTmmX_r9pE_eg-6tyiylj5I9hOpgUMtogAgRSNA8VP5YLvoDv5D3eMhK_ZzTQtQGEQulpA86uPKjImusrAe4XAbFEfWIPZ--S6xkYacgCzGjqfAQOInmRLg_fOcmuy2atMbCX9Rf66rbGhOTwIY-HEBUAeIA9cY_AL-rb78ErzcKhRodnAN3XXq-rpA9709UjBiFm_SEPGEsA6HlmxDoPFubEt1g-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:

m0uVEEEqSLHJRbG-xLOsyA

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

eyJhbGciOiJSUOEtTOFFUCOyNTYiLCJlbmMiOiJBMjU2RONNIiwia2lkIjoiNmEyYmNkO DgtYTq3MS00MjQ1LWEzOTMtMjq0M2VhZmU2ZTAyIn0.lRs vcZlauJs4VwED3wZGr3wJDbq8It9 zBStuJqqf7TiGs3kUCSulPwA6jRA-8xuHTpNtKr1w0hsNbUhsx-3BL5zGaDzsSekA1AZVevVy2qOrfId6OxLOb81SpVnSRR K3jRHDWfH ZDqZqMoM2mv6qFvb8GqG FV59 jIkhctX73Y6iqe3NCask2CT0Ine3SUFVxt OBqnBCwgDLrauGyisQbpVN1JJRjsWPeyXA0 OWvlECnRSLS93-prnMrfLTU JHUyU304-cq7qVu7OATP1NB78L8m0-MiIF tr0mpbaEneOLDbimNYt2UVgn1thJsvh5Na30GKY5t-ISHoWhX-DvVHp3KTEpp0bkC8IczZt-jq-2vdYhyM7Sz1H0c9w2EvSSryYsAVonOojl4yWeaNhP 7mk09hgu1MUkr91Tfr-U1k3zFHyCClfJzHj3t3uebS2mFDEyuao7K4omC335 VYsCi6kRSU421AW1 8V21RxaS2VDBQbgo Cqr3UQQxsoSRIG3v1-OBgTgZ9slEGZnEihaptab-7IeqnXIbhZNA8OnzyOwKW2S6r8M2eDd01QhGaDPGXcdWtOpC-Qcvu9MJTp4MRDx5dYe2rRQaI A7WS5vJGkjwdRRpfhaJhGoXA7Wc6eUmB UFOvPfsGQdFXPBUB3v h6jPfsER6hnXjU.75ZoCOOVRqIWRyAs.GiB15WaorEeK77gX1Tr-141X0520tRcvrhp8D9cHCfYLTIonEo3MXYQ46Z8QTPv2ueCdiKztQDngTuczGGY31ve1cztHqeAJZ92UG9cjouMVE7IY29ML7OrzPy66GJsVb3BZnmIm6vDNEMf9AL8LH3y-H4rk9JmZjQbrRIU2AbmTGwRK0 FnQD660b-4nEMKfc51h9bkdc8as3 OxFH2b0KxaiZDki8pDLumCFPQ9U9pfU7KUmkF1O9FGF3FpryGX5DzEE YprotK6lcEr9 f8U5ooHS PF06pprnL CkXtimdJEnJgghk-5XdZfdIMIR4ghYPDT rfE0GjmroEaWOaoM3qXwDhdUFs1nb 48KAUOQY1ebgd9Ngi edrh517TAj1wPCmqnPEY9SYIPeorurSwlMPPpI9NN-bjjBUhW1a4RxkCt5UeHDS-bvRkPqD5DaiOQq2RD7n8cm6pzHKcKO16WpXSSFhIjK1l kevoprXPIEHtWik3PBSXYWDz15Gc ET-aw2CF6xgWkUivw512 ySvs66grxGqubBQkOOxLLyUEmcxedPSCSs6g4eNqf-SES0yZ9NR4uBs3WBsqs2h0Ftrn5ZKniMDQKtoU0LJvscjXBso6ckAVuvjBilY4zKqr07FjJ9zn-9xkStotxms0czBofOsVunTuKypLBvTiwV4uykgUnsxbyOtuUvr10kLK1dma4F9q1qixRqfoMyn1o7seRDTRrTkBh D AzNhZG3o1TC5bHUtwN5crc2dw3FkS4UMe1unQkusFL44MRqY3qbn iP4NY8X3bWTWtp31kiFxKt ATTiZG lvi5omlQwcA7a mYQw47EjjvGTiSJQsfDM8d2WBlVDOV65xqcqy70QVRPxfTo6jJu-X1MGd-RN2Lb crLsnJGJ6kpdhqyF7ts 3qbWvryzKLJyDe2HM3izN6Kw0U4Ba- YOMPVmJECsVC5KUw9jRYhw6tdYSU41LXKRDnMyhcjRyuv4V347DOR280aGWsbqpqaDp4mdtkaABARhtO5BhbzzeSnHnEjTVZmdn8H5WifzGvqHCiGA

z752CNNO000wCbpVoW2Jcq78XndubsxsXzkcq0XvsDxnKzdBdRkoYyTEd5tMOdxUZw tpbXNQZF

RC TICS.IS v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



FwAB4ph_FtoYC0j50kGhEola6h7jguoFJu0CewloGSkvvqu2Ht4G9IfDkFs0tMTvdjHJJGWpDj9nQ_Mzn0QkKBPhGLM50yUtosIVd1FvrHCJuhkt3qsAP6OTHvgDswELnLMcOsoRB2qdVp6YSAOT3ZuRc6Bawwd5S78wd_o4ISW9pNMxNbHPueiXI_N48S9Zcb2ktwH6dB3rbkRwgXCEWcPheX8s5ik325PbY5RAs29fj45yISSZ-

6xlg9BwBXjg81TkNg18_6j0aI8ZZmDjL1EyjK0ojb9UpQUfjreakNAGhxSa5S_ethmI63Bs6_En XyzOKDP5sPmlyBgJ6RjXRSmVI8zqA1ETazPY93PYql_PqADQm48_Ocs1h_djjNNBHeA8ucYelX1 T8tcD-ENwrvJw8 2u1A1DWX-

FucPGQQLZc4PkwO4OCUeBlxDUsJFzedhX0cKEQr_b9zxhVT3C09yr3q6FyhqrYF892Kq106PmXBVEZrb-Q0piVZyozeordNJGRE016r8A10hnc-KgUlkdZrxee zzk9aV08CU01-

fvBRCGOR12v EAcY17pnyfnCKmZH3u3Iq5D7-

T3JHJSZz2NuUFrCok81L87X0YbRCscW164VAEsF1QolakktKt8cNRQwj_95rtt1Ka06Fdg6Q-VK9NskncKRKnlWcIQT6Ec6eTmr1Ng7JaQ7dqkEh zThM8ifE-

Ak6jVdpMiHZ4NvdlOndCPbi1r7zFNrUeRI0BK5PWfOJA90YAnMJ3B7DkrAMyLhZMkKXp4UjEZSQ hBhe lnD9VxL3rZcmRqEctFVmsTnyRZY-

pZlsx8gS__99WXrtNqD1lR3njeHWJsCi35GoJJwWh3BFCJvsyeQcmsIkkN4RdBrwj_B-ZpUKJn1gvho2E7PPkvuMpMPSWr1c1zptCpzamAY2pTjBgmQ5NWDnxN87fUZN9YaJYMcqD7kb-kooJuNWw7TcF-YPo 31UHHWd3mKzBVFUeYEqqJBA-

9KroMQzfC7hc5QQkaA_oGVn0_8_AexX7fNDdXc6yRzM_msfGsbO6pMYegbEijS5F3DaopvpAmwdBbFlDRUIGSKpfODn9DNGB2BoqNn1mNPCuBsqGuPvF3RzgxP-1MoCI3Xf7RxG1DYr-

bTPsV6pyzinV5HaGSNRorYkXchaXhl19k4d9pfu_4uXeASFVG6WxzdpVwb_w769VQdVYL7KG0u4uC_MhWDH0w1DVEFySffBNPpZ6Z_lLYkbc8epocBH9HjJVFByP4gqVieVuDlX_tkK6QUwSPZTl36Be4uVf9luAJXZfn3IkMbj8KuRfLjwBE3N4MnjXbz4RHN5dZwaSJftRgYo_DaJPiqcGz1H3dB5B4i0A7bLA4H1TEIKLPom-

A1GnpRruGdoF7dD3dhx8HOKUt7ny7zMrYQWI86bmRzubnMZmi87GguvCoCP7o7ATMJIGprSDmg-3TJ5FGyeXaNRZO1EP1Dhc6uh19Pm_PYP718tKg5Z_dGgnFWwJp2SDweU7kvWgEUePJVa-HKd7iiRGP-

2cttS8ak4zlq_OjKkFRHi6A2uZ95Yg0dkWgBbHgCHbbuM5oBmIztFixmnHeoTrV3HPbBPw2jEX_XINhFVcYnfc1efs0Gh-

jKA4wrCgStq5bXRhMC5degaoQ0Sb5eY_S_Ehpz1yoA_JYDHp6t8FfnSMTNbM9LfoBTgZDdlrRmwd2dBVJxzkbhTpXo4dpShFRsL1vs0GV3wdELBuzMb3UaTyu-

rJy_DOblfPE8pmlC1NS2_WHrVXB0gJf91MaaIup_Fx7tJzSbqiNG9mFj6SQvMk0HvAyI195NpyFNX33x5NLFnF6125mZdn6MY6nLPeNu9P1yEadZ8uXnMtwfrAOuN83yS2XZDWKHPYSJOaVcsGAjRrcGLpulp-dcx1g0XVQgNR0KzaH7J3zbRJ-Lqf7V6w9aYT1JnHk21bof2oGp9NaWN1-Tq1OEvrAk3-

EqzyCigOG5A2YZdoRR_1rlCxfNCXz0dtRwM07IX_kEEEKHTs41k970YTSa_SdhYNMUN0QPBLkjTts_YMnx8Y2wFumFy9Ji3K5o2GHB5nc0a1DioSi9gNEpFjv6pT_Tk9NDIFUBAwv8oV_qp41qFqSpA9g6G51madn0K6sonvAsRlDWNjxSBropg1stgWWCRe3Ucp_b9PhZht1rSuJsZynEqLCf9ZLn2lxfugLbIOdvaNZxkI2NtNHCv_CsiMFo76rC5SwCJ5uTtD64z53s2txbOPmhWpIGE63OKi3fQSZz5HZdBbidIRcM3vCEseMNw1A27F7BCIN6o9tZd-1X0Zkvh08Wts2d-c1Fs-

x5ssLWeoMPpGvnFjZ9pQBD8EyK34JsA5qPTVjLOD62ZRph8PdkiJIoE0es4QMyleVbUe9rbscIN F2m5YSHiRWWM5MFSpDFmT67EtriseeWQnVNQTU31_chDRut92yv2G3seSa8HHMLW0Gmq7W7hUUG uxLbUSVv74U7 55vpQM0fuRhJ7khTbZioN-

wBp32Zyy_phgMi5sOqV35lPoCzpZ7ueQwbsS6kvABCj2PjoeQL2trqrjcfkPfLPUKsETgkVrgvijt55bzKmUG624fv1zJbgSt7t3rrPiVQyKflW0YJcx-

fH55R2sS4GVw74DfWF1k7wp9Upw3JjlgQ9MhRpVjUd98CprL-

jjdn4k4CuHxZPXEoXEfkvC8PO4HmDN1Od-

3ShVrilhJ1gLFpuM1814OylUju9bhHEM8R28YL7ftgWvtzhMkdw3BPM05Uzo29xAsS_GZeDikFldb2E7CoZu3evhnrMsk9KWGbbrxcAZDFR1zhNJHJBFVPpjpxgoXy6Br3LAtZBnu217Zt5mfAF08hEG0baz-MS0hPahcfoE3S7c5xPcV4wTmmX r9pE eq-

6tyiylj5I9hOpgUMtogAgRSNA8VP5YLvoDv5D3eMhK_ZzTQtQGEQulpA86uPKjImusrAe4XAbFE fWIPZ--S6xkYacgCzGjqfAQOInmRLg_fOcmuy2atMbCX9Rf66rbGhOTwIY-HEBUAeIA9cY_AL-rb78ErzcKhRodnAN3XXq-rpA9709UjBiFm SEPGEsA6HlmxDoPFubEt1q-

RC TICS.IS v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



36CxG410LaKSEAXPUm105xNWUHS_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 امضاشده و رمزشده را تولید می نماید:

```
/** 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();
```

RC_TICS.IS_v1.4

سند « دستورالعمل فنی اتصال به سامانه مودیان »



بهمن ۱۴۰۳

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

jwe.setAlgorithmHeaderValue(KeyManagementAlgorithmIdentifiers.RSA_OAEP_256);
jwe.setEncryptionMethodHeaderParameter(ContentEncryptionAlgorithmIdentifier s.AES_256_GCM);
jwe.setPayload(signedJson);
jwe.setKey(publicKey);
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 صرفا به منظور آشنایی دقیق تر با فرآیند تولید بسته ی امضاشده و رمزشده ی صور تحساب می باشد. در این بخش هم برای عملیات تولید JWE و JWE از کتابخانه jose jose نسخه ی methand Met

```
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());
```

RC TICS.IS v1.4

سند « دستورالعمل فنی اتصال به سامانه مودیان »



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 صور تحساب 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" />
```

٧- ١- 4- ارسال صورتحساب

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

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

ىند « دستورالعمل فنى اتصال به سامانه موديان »



Send Invoices – ارسال صور تحساب	
https://tp.tax.gov.ir/requestsmanager/api/v2/invoice	آدرس
POST	Method
لیستی از InvoicePacketها هر یک شامل موارد زیر:	
• Json آبجکت header: آبجکت header	
o requestTraceId: شناسه منحصر به فرد درخواست از نوع	
o fiscalId: از نوع رشته، شناسه حافظه صادر کنندهی صور تحساب	ورودى
• payload: از نوع رشته، بستهی JWE صورتحساب (امضا شده و رمز شده)	
محل قرار گیری: Request Body	
در یک درخواست ارسال صور تحساب امکان ارسال حداکثر ۱۰۰۰ صور تحساب وجود دارد.	
آبجکت Json دارای فیلدهای زیر:	
• timestamp: برچسب زمانی لحظه ایجاد جواب	
• Ison هر یک شامل شیئی که دارای فیلدهای زیر است:	
o uid: همان requestTraceId ارسال شده به ازای هر صور تحساب	خروجي
packetType o در اینجا null است.	
referenceNumber : شماره پیگیری صورتحساب ارسالی	
o data: در اینجا null است.	

با استفاده از این API شرکت معتمد می تواند همه ی صور تحساب های مودیان مختلفی که دسترسی ارسال صور تحساب را به شرکت معتمد واگذار کرده اند ارسال نماید و نیازی نیست همه ی صور تحساب های موجود در یک در خواست متعلق به یک شناسه یکتای حافظه مالیاتی باشد. همچنین مودی می تواند در یک در خواست ارسال صور تحساب، صور تحساب های مربوط به شناسه یکتاهای مختلف خود را ارسال نماید. البته شناسه یکتاهایی که اجازه ی ارسال صور تحساب 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 درصورتی 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 RC_TICS.IS_v1.4 بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



یکتا برای دو صورتحساب از requestTraceIdهای تکراری استفاده نماید هنگام استعلام وضعیت صورتحساب با uid تنها یاسخ وضعیت یکی از آنها به عنوان جواب برگردانده می شود.

نمونه در خواست cURL ارسال صور تحساب 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 ]...EEzZe9mxIxw",
        "header": {
            "requestTraceId": "cf019c26-f235-11ed-a05b-0242ac120003",
            "fiscalId": "A11216"
        }
    }
    ]'
```

در صورت صحت توكن و درست بودن ساختار درخواست خروجي برابر است با:

استعلام وضعیت ارسال صورتحساب - استعلام

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

RC_TICS.IS_v1.4

ىند « دستورالعل فنى اتصال به سامانه مودمان »



بهمن ۱۴۰۳

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

استعلام صورتحساب به وسیله شماره پیگیری -1

به وسیلهی این API می توان وضعیت صور تحساب ارسالی را با استفاده از کد پیگیریای که وب سرویس جمع آوری به ازای هر صور تحساب 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
فیلدهای زیر:	
• referenceIds: لیست شمارهی پیگیریهایی که قرار است استعلام شوند.	
 start: شروع بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 	
2023-05-14T00:00:00.00000000+03:30	
 end: پایان بازه زمانی که در آن به دنبال صور تحساب هستیم. فرمت: 	
2023-05-14T23:59:59.123456789+03:30	ورودى
ورودیهای start و end اختیاری هستند و در صورتی که مقدار دهی نشوند، جستجو در بین	
صور تحسابهای ارسالی در ۲۴ ساعت گذشته انجام می گیرد. همچنین بازه زمانی مورد استعلام	
نمي تواند از يک هفته بيشتر باشد.	
محل قرار گیری: Request Params	

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



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

- referenceNumber: شماره پیگیری درخواست استعلام شده
- uid: شناسه در خواست (همان requestTraceId که صور تحساب با آن ارسال شده بود)
 - status: وضعیت صور تحساب دارای حالتهای زیر:
- SUCCESS: صور تحساب فاقد خطا بود و با موفقیت در کاریوشه ثبت شد.
 - o FAILED: صورتحساب ارسالي داراي خطا بوده و رد شده است.

خروجي

- o :IN_PROGRESS: صور تحساب ارسالي هنوز در صف بررسي مي باشد.
 - o NOT_FOUND: شماره پیگیری داده شده یافت نشد.
 - data: لیست خطاها / اخطارهای موجود در صورتحساب
 - packetType: نوع بسته
 - fiscalId: شناسه حافظه ارسال کنندهی صور تحساب
- sign: امضای پاسخ به فرمت بسته ی JWS که ساختار آن در جدول بعدی توضیح داده می شود (فقط در حالت SUCCESS)

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

	امضای پاسخ نتیجهی اعتبارسنجی صور تحساب - JWS	
	یک شیء JSON دارای فیلدهای زیر:	
	• alg: الگوريتم امضا: RS256	
	• sigT: زمان امضای تو کن	Header
	yyyy-MM-dd'T'HH:mm:ss'Z' 2023-05-13T10:44:47Z	
	شیء JSON دارای فیلدهای زیر:	
• referenceNumber: شماره پیگیری درخواست صورتحساب ارسالی. مثال:		Payload

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

ىند «دىتورالعل فنى اتصال بەسامانە مودمان »



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

• clientId: شناسهی فرستندهی صور تحساب. مثال:

A1112K

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

A1112K04D1271489087018

• receivedDate: تاریخ دریافت صور تحساب در سامانهی مودیان. مثال:

2024-01-08T11:38:54.388Z

امضای بسته ی حاصل از الحاق Header و Payload با استفاده از الگوریتم RS256 و با

استفاده از كليد سازمان.

Signature

شما می توانید صحت امضای بسته را با استفاده از کلید عمومی سازمان (دریافتی از متد Get) (Server-Information) اعتبار سنجی نمایید.

ر نمونه دادهی امضا شده هنگام استعلام وضعیت صور تحساب:

eyJhbGciOiJSUzI1NiIsInNpZ1QiOiIyMDIOLTAyLTEOVDAzOjA4OjM5WiJ9.eyJyZWZl
cmVuY2VOdW1iZXIiOiIzMTk3NzhlMC03Zjg0LTQyNDktOThmNC1kZTc5OTBjYjdjNjkiLCJjbGl
lbnRJZCI6IkExMTFPSyIsInRheElkIjoiQTExMU9LMDREMzYxMjAwRThEQjIxNCIsInJlY2Vpdm
VkRGF0ZSI6IjIwMjQtMDItMTNUMTE6NTI6NDIuOTgyWiJ9.lanl052gttnAp6F1MX9NxPn9swN4

IjFiowTX2ytm_1YgAqgzBLytvTBRrq_NopeIH9LIRd275iFJaysMxbFmVnstTLp91hG_iMGFFQv
AXxwY5EL LYnexu-

biPSswfTXK9lf6RjKrIIDm0hyBr2pCZpc_ZXSgwLHyaf1p_GgxvYSql4l3xCNzzFKfp3yI8r0Pa hIHovmUlkbdriH_YXKckDw9ZlH6a3NcVslmj65Ed7pemBMmJLPf_Kj7tn7e8s4dUGh0fs6HEotY fCB7LMDejPDu6jgbIPkwANHWAxx3dZOeO3bUKSo6SIyInvo3GQvDP5dpyGngkQ9NAme7HKg-HjDHJJzEcjKACG-

Gj3LEsyQveHrL4s5q9YGYWwavZVinbTRMwl75_LRgIeB1UuWNVLS5PtSk2o6drzRnNJ6iN542HH tOvnF_y8J57oO1LHXDtpMS5ncQF2e_NJ2tGmFxQs868T1ODgqaHzBc3H7VyQ8KC1uD_W3zAf93e 1ErKbAdVt2eDHZVFHoREZVoYW3m7qraO5fiYcYUle9TUXLARQwd_ihEcKbRtLbtw42ZHqfXZe52Q77vJdY79Xb8OkUjA5kfJ6g4o80Qqa-NaIoeWrFte0g5e-

 ${\tt SUSJklnd4pZTTApZfCMOngoKFSGJ0USfi0T3M-OX7lyxJbOYKeqUzt4}$

نمونه درخواست استعلام وضعیت صورتحساب با استفاده از شماره پیگیری:

```
curl -X 'GET' \
    'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-reference-
id?referenceIds=f9173085-2316-4ca6-918e-e41aaf7ef8dd&referenceIds=93367b02-
23dd-4568-90e1-2b47d799f361&start=2023-05-
14T10%3A00%3A00.000000000%2B03%3A30&end=2023-05-
14T21%3A00%3A00.000000000%2B03%3A30' \
    -H 'accept: */*' \
    -H 'Authorization: Bearer eyJhbGciO...[ JWT TOKEN ]...q4RcXogA'
```

در صورت صحت توكن و درست بودن ساختار درخواست خروجي برابر است با:

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

RC TICS.IS v1.4

سند « دستورالعمل فنی اتصال به سامانه مودیان »



بهمن ۱۴۰۳

```
"uid": "2b982bfd-9a60-47cd-9da7-30fc0dabd37d",
    "status": "FAILED",
    "data": {
      "error": [
          "code": "012802",
          مجاز مقادیر جز «تسویه روش» فیلد در شده وارد مقدار": "message"
,".نيست
          "errorType": "ERROR"
        }
      "warning": [],
      "success": false
    "packetType": "receive invoice confirm",
    "fiscalId": "A1110K",
    "sign": ""
  },
    "referenceNumber": "f9173085-2316-4ca6-918e-e41aaf7ef8dd",
    "uid": "c5352f85-9322-41bc-a5b2-9abb130fe622",
    "status": "SUCCESS",
    "data": {
      "error": [],
      "warning": [],
      "success": true
    "packetType": "receive invoice confirm",
    "fiscalId": "A1110K",
    "sign":
"eyJhbGciOiJSUzI1NiIsInNpZ1QiOiIyMDIOLTAyLTEOVDAzOjA4OjM5WiJ9.eyJyZWZ1cmVuY
2VOdW1iZXIiOiIzMTk3NzhlMC03Zjq0LTQyNDktOThmNC1kZTc5OTBjYjdjNjkiLCJjbG1lbnRJ
ZCI6IkExMTFPSyIsInRheElkIjoiQTExMU9LMDREMzYxMjAwRThEQjIxNCIsInJlY2VpdmVkRGF
0ZSI6IjIwMjQtMDItMTNUMTE6NTI6NDIuOTgyWiJ9.lanl052gttnAp6F1MX9NxPn9swN4-
IjFiowTX2ytm 1YgAqgzBLytvTBRrq NopeIH9LIRd275iFJaysMxbFmVnstTLp91hG iMGFFQv
AXxwY5EL LYnexu-
biPSswfTXK9lf6RjKrIIDm0hyBr2pCZpc ZXSgwLHyaf1p GgxvYSql4l3xCNzzFKfp3yI8r0Pa
hIHovmUlkbdriH YXKckDw9ZlH6a3NcVslmj65Ed7pemBMmJLPf Kj7tn7e8s4dUGh0fs6HEotY
fCB7LMDejPDu6jgbIPkwANHWAxx3dZOeO3bUKSo6SIyInvo3GQvDP5dpyGngkQ9NAme7HKg-
HjDHJJzEcjKACG-
Gj3LEsyQveHrL4s5q9YGYWwavZVinbTRMwl75 LRgIeB1UuWNVLS5PtSk2o6drzRnNJ6iN542HH
tovnF y8J57o01LHXDtpMS5ncQF2e NJ2tGmFxQs868T10DgqaHzBc3H7VyQ8KC1uD W3zAf93e
1ErKbAdVt2eDHZVFHoREZVoYW3m7qraO5fiYcYUle9TUXLARQwd ihEcKbRtLbtw42ZHqfXZe52
Q77vJdY79Xb8OkUjA5kfJ6g4o80Qqa-NaIoeWrFte0g5e-
SUSJklnd4pZTTApZfCMOngoKFSGJ0USfi0T3M-OX7lyxJbOYKeqUzt4"
```

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

uid استعلام با −۲ -۸

شناسه سند RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



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

Inquiry by uid – استعلام به وسيله شناسه درخواست	
https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-by-uid	آدرس
GET	Method
فیلدهای زیر:	
• uidList: لیست شناسه درخواستهای صورتحسابهای مورد نظر	
• fiscalId: شناسه حافظه صادر كننده صور تحساب	
 start: شروع بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 	
end • یایان بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: 2023-05-14T00:00:00.000000000+03:30 • 2023-05-14T23:59:59.123456789+03:30	ورودی
ورودیهای start و end اختیاری هستند و در صورتی که مقدار دهی نشوند، جستجو در بین	
صور تحسابهای ارسالی در ۲۴ ساعت گذشته انجام می گیرد.	
محل قرار گیری: Request Params	
دقیقا مانند استعلام با شماره پیگیری	خروجي

نمونه درخواست و پاسخ این API را می توانید 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 توكن و درست بودن ساختار درخواست خروجي برابر است با:

RC TICS.IS v1.4

سند « دستورالعمل فنی اتصال به سامانه مودیان »



بهمن ۱۴۰۳

```
"code": "011107",
          شناسه/ملی شناسه/شماره» فیلد در شده وارد مقدار طول" :"message"
مقدار طول) .است مجاز طول حداکثر از بزرگتر «خریدار فراگیر کد/مدنی مشارکت
" (باشد 10 حداكثر بايد شده وارد
          "errorType": "ERROR"
      "warning": [
          "code": "111208",
          «خریدار اقتصادی شماره» فیلد در شده وارد مقدار طول":"message"
,"(باشد 14 حداقل باید شده وارد مقدار طول) .است مجاز طول حداقل از کوچکتر
          "errorType": "WARNING"
        }
      ],
      "success": false
    "packetType": "receive invoice confirm",
    "fiscalId": "A1110K",
    "sign": ""
 },
    "referenceNumber": "60e834f9-14b6-43be-8b77-85471678d3da",
    "uid": "cb080c58-e36f-4bb0-a932-90f672109fb6",
    "status": "SUCCESS",
    "data": {
      "error": [],
      "warning": [],
      "success": true
    "packetType": "receive invoice confirm",
    "fiscalId": "A1110K",
"eyJhbGciOiJSUzI1NiIsInNpZ1QiOiIyMDIOLTAyLTEzVDEyOjAxOjExWiJ9.eyJyZWZ1cmVuY
2VOdW1iZXIiOiJmMWQyMDYwZC0zMzZkLTQwNDUtYjq2ZC03ZTAwMTUzOWQyZTUiLCJjbG1lbnRJ
ZCI61kExMTFPSyIsInRheElkIjoiQTExMU9LMDREMzY3MjJEMzk2QzQ2MyIsInJ1Y2VpdmVkRGF
OZSI6IjIwMjQtMDItMTNUMTI6MDE6MDcuODkOWiJ9.PKlMMmvlU6aVsB4u6CvVD4UANik5QFmlo
tsnil9EwOiEBTLpn 2S0bkBN5CecIGDX7abRMr8X3H385 gE1oglCv F7e-
r5JVzQVbks82AFhUGkT09AGjhTqTQk45MvtOY1mb26YgsWovERPy4ApgINLUwJH9Pw4otnorHI
eNgnu- -JKTVPul4mnfTFMeb7PTDUyv9uIbpwaR5BbVL8OPtL6J4RAl5lI-coTLnCUMi9LLj-
rUDVkHjdf3 NPL7NADA4GvZwgFZ3Fv2sZxete8z7DBuN4ZdNhvpbs9fYlqdwEkoTE2ZsqD9XapE
\verb| 1UMDCQt8oAGG4G2W0JInb30F2ZrSqq2UaVSZ30iCZFbJ8qXoG1X7IomcgCJ2Bs991c4umrn78Mx| \\
2s2UFiF9ckkfJgsIUgpk3jeQ8oEVJuLCRoeTA5MmP4j3Z z2AFDzkazhZAXmGfDtp6O80HHKz4K
pm77ccTgIPiIYZawb5VUZe1OdOdguFb2T2q3aeP7bA91ue4ntmYaL19vjaEhi7XI5XdbH189t7x
20aHx DR70h2KI9hbFZBSEZJM JmXPDJ6slhFvHcblMPf-
p9fT2r3NOj5mNiBUREnTLi6NvUXwUz6hhspdvdE-xrW51aMkGPp4 Zy51YNKi9KZ1d EWhMpwe-
HtQjXeVEyc8ldkE4uSP6IE"
```

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

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



- استعلام براساس بازهی زمانی - استعلام براساس بازه - ا

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

Inquiry – استعلام در بازه زمانی	
https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry	آدرس
GET	Method
فیلدهای زیر: • pageNumber فیلدهای زیر: • pageSize: شماره صفحه (مقدار پیشفرض: ۱) • pageSize: اندازه ی صفحه (مقدار پیشفرض: ۱۰ – مقادیر مجاز: ۱ تا ۱۰۰) • status: وضعیت صورتحسابهایی که به دنبال آن هستیم. • SUCCESS, FAILED, TIMEOUT, IN_PROGRESS: • مقادیر مجاز: Success, تحالی باشد همهی صورتحسابها بر گردانده می شود. • در صورتی که این فیلد خالی باشد همهی صورتحسابها بر گردانده می شود. • start: شروع بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: • 2023-05-14T00:00:0000000000+03:30 • نایان بازه زمانی که در آن به دنبال صورتحساب هستیم. فرمت: • 2023-05-14T23:59:59:123456789+03:30 • ورودی های start و end اختیاری هستند و در صورتی که مقدار دهی نشوند، جستجو در بین	Method
صور تحسابهای ارسالی در ۲۴ ساعت گذشته انجام می گیرد.	
محل قرار گیری: Request Params	
دقیقا همانند استعلام با شماره پیگیری و uid	خروجي

نمونه درخواست ارسالي:

```
curl -X 'GET' \
   'https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry?start=2023-06-
10T00%3A00%3A00.00000000%2B03%3A30&end=2023-06-
10T23%3A59%3A59.9999999982B03%3A30&pageNumber=1&pageSize=10' \
   -H 'accept: */*' \
   -H 'Authorization: Bearer eyJhbGciOi...[JWT TOKEN]...iKKXzBjRZw'
```

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

RC TICS.IS v1.4

سند « دستورالعمل فنی اتصال به سامانه مودیان »



بهمن ۱۴۰۳

```
"referenceNumber": "780c7cb1-84cf-4df8-a87d-160448f38c55",
    "uid": "b3bd6327-1c57-4cae-85ed-5c88de28aea3",
    "status": "FAILED",
    "data": {
      "error": [
          "code": "011107",
          شناسه/ملی شناسه/شماره» فیلد در شده وارد مقدار طول" :"message"
مقدار طول) .است مجاز طول حداکثر از بـزرگـتر «خریـدار فـراگیر کـد/مـدنـی مشارکت
," (باشد 10 حداكثر بايد شده وارد
         "errorType": "ERROR"
      ],
      "warning": [
          "code": "111208",
          «خریدار اقتصادی شماره» فیلد در شده وارد مقدار طول": "message"
,"(باشد 14 حداقل باید شده وارد مقدار طول) .است مجاز طول حداقل از کوچکتر
          "errorType": "WARNING"
        }
              ],
      "success": false
    "packetType": "receive invoice confirm",
    "fiscalId": "A1110K",
    "sign": ""
  },
    "referenceNumber": "60e834f9-14b6-43be-8b77-85471678d3da",
    "uid": "cb080c58-e36f-4bb0-a932-90f672109fb6",
    "status": "SUCCESS",
    "data": {
      "error": [],
      "warning": [],
      "success": true
    "packetType": "receive invoice confirm",
    "fiscalId": "A1110K",
    "sign":
"eyJhbGciOiJSUzI1NiIsInNpZ1QiOiIyMDIOLTAyLTE3VDA5OjA3OjUzWiJ9.eyJyZWZlcmVuY
2VOdW1iZXIiOiI4MjczYzhkMi1jNWJmLTQyYmQtYTQwZi0wNDA1MjA5YzU2MjkiLCJjbGllbnRJ
ZCI61kExMTFPSyIsInRheElkIjoiQTExMU9LMDREM0FFQjM1MjAxQTc1NyIsInJ1Y2VpdmVkRGF
0ZSI6IjIwMjQtMDItMTdUMDk6MDc6NTEuNDUyWiJ9.VnC48sJLngr2YqjpD50bHYmBP0oIZP-
KK7CxB9aZjTPAU5x4xKSyYdCNGRfWlLmnHRpVAHUKs3oeRsHF uxfD2nGDC6qXHg6MFOcnLU3Hc
IETk-tqIqyVRv3eO6zMyf9ImjatQkD-niW0wjyk7YkK wl3XFy7lve4YMnR2yE49V-
1ejjj1CwlnICyVlMKG-
IkpnGNv76HA3V0mPZ7Jtlb2cSFt037WVkD9eAGMS18biOYXsPHgsu1f1USHIrgAWCGagOfkp gF
C2nHC4um8RXGAKfxqBQTbmvSEOEk7R3dxRsciNSsxseS9QZIDJqMPmxZcOZFjT0H5Gt8Kpqj2qj
3LcVxXyk3R QGH1w8FhLU8SAECCnLtkPazZ8I WHnSAOwXvV N3qKB5QkCLK-
8No2LPvktsuDT1R5-GB8wI2cTsxsRuG9QI0MCKBvbGVntSR5oEA UgP-
pT70MXswFsvkoCAmkEfRagor0-
IFzNU6z2NVy8bNZ4snwp8VaQNbqXqxuncUVikdoUsbC uT648alq6QZw4xDeRCbt29Ut9VNY91S
UT9s5BCnyS1B-
```

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعل فنی اتصال به سامانه مودیان »



6fk4IhQUO8KkpD37HMTCTNHur33dFQ_qDHG4zcttGI1Q4lj7f6FwP8c1wW59oVCAJfLyekJjGr5
a0aqJtQXF3G5YwBzfQmtRj6hP62cyWC5ixv8"
}

9 - استعلام اطلاعات حافظه و مودي

9- 1- اطلاعات حافظه

این API اطلاعات مربوط به حافظه مالیاتی (شامل فعالبودن / عدم فعالبودن، 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	
https://tp.tax.gov.ir/requestsmanager/api/v2/fiscal-information	آدرس
GET	Method
• memoryId: شناسه حافظه مورد نظر	
محل قرار گیری: Request Params	ورودى
شيء JSON شامل فيلدهاي زير:	
• nameTrade: شناسه حافظه	
• fiscalStatus: وضعيت حافظه	خروجي
• nationalId: شناسهی ملی پرونده / کد ملی صاحب پرونده	
• economicCode: کد اقتصادی پرونده	

نمونه ورودى:

```
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 توكن و درست بودن ساختار درخواست خروجي برابر است با:

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

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

ىند « دستورالعمل فنى اتصال به سامانه موديان »



9- ۲- اطلاعات مودي

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

GET Taxpayer – دریافت اطلاعات مودی	
https://tp.tax.gov.ir/requestsmanager/api/v2/taxpayer	آدرس
GET	Method
• economicCode: شماره اقتصادی مودی	
محل قرار گیری: Request Params	ورودی
شىء JSON شامل فيلدهاى زير:	
• nameTrade: نام مودی / پرونده اقتصادی	
• taxpayerStatus: وضعیت پرونده شامل فیلدهای: «NOT_ALLOCATED» به معنی	
تخصيص نيافته، «ACTIVE» به معنى فعال مجاز، «DEACTIVATED» به معنى غيرفعال	
(عبور از حد مجاز ماده ۶)، «TEMPORARY_UNAUTHORIZE» به معنی غیر مجاز موقت،	خروجي
«PERMANENT_UNAUTHORIZE» به معنى غيرمجاز دائم و «PERMANENT_UNAUTHORIZE»	
به معنی مشمول تبصره ماده ۲ میباشد.	
• nationalId: شناسهی ملی پرونده / کد ملی صاحب پرونده	

نمونه درخواست ارسالي:

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

در صورت صحت توكن و درست بودن ساختار درخواست خروجي برابر است با:

```
{ "nameTrade": "انزلى آزاد منطقه ايرانيان الكترونيك پيشخوان",
"taxpayerStatus": "ACTIVE",
"nationalId": "14003778990"
}
```

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

ىند « دستورالعمل فنى اتصال به سامانه موديان »



10- استعلام وضعیت صورتحساب در کارپوشه

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

GET Taxpayer – دریافت اطلاعات مودی	
https://tp.tax.gov.ir/requestsmanager/api/v2/inquiry-invoice-status	آدرس
GET	Method
• taxIds: ليست شماره مالياتي صور تحساب	
محل قرار گیری: Request Params	ورودی
شىء JSON شامل فیلدهای زیر:	
• taxId : شماره مالياتي ارسالي	
• invoiceStatus: وضعیت صورتحساب دارای مقادیر زیر:	
REJECTED(د شده)	
APPROVED(تاييد شده)	
SYSTEMIC_APPROVED(تایید سیستمی)	
IMPOSSIBLE_REACTION(عدم امكان واكنش)	
(در انتظار واکنش)AWAITING_REACTION	
NO_NEED_REACTION(عدم نياز به واکنش)	
CANCELED(باطل شده)	خروجي
DELETED(حذف شده)	
SYSTEMIC_REJECTED(د سیستمی)	
• article6Status: وضعیت عبور از حد مجاز ماده ۶ دارای مقادیر زیر:	
EXCEEDED (عدول)	
NOT_EXCEEDED(عدم عدول)	
• error: خطا، دارای مقادیر زیر	
NOT_FOUND(صورتحساب یافت نشد)	
(دسترسی ندارید)ACCESS_DENIED	

نمونه درخواست ارسالي:

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



```
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 ]...klQXOM-_uA'
```

در صورت صحت توكن و درست بودن ساختار درخواست خروجي برابر است با:

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

11 - پیوستها

11-1- گواهی و کلید خصوصی امضا

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

----BEGIN CERTIFICATE----

MIIDejCCAmkgAwIBAgIUV27QXqJjK2EgFy9zeYkpsX+ISPswDQYJKoZIhvcNAQEL BQAwcTELMAkGA1UEBhMCSVIxDDAKBgNVBAgMA1RlaDEMMAoGA1UEBwwDVGVoMREw DwYDVQQKDAhNb2hheW11bjEMMAoGA1UECwwDVGF4MSUwIwYJKoZIhvcNAQkBFhZtLm1hbHZlcmRpQG1vaGF5bWVuLmlyMB4XDTIzMDMyNDEzMjgyM1oXDTI0MDMyMzEzMjgyM1owTTEPMA0GA1UEAwwGQW56YWxpMRcwFQYDVQQKDA5RdW9WYWRpcyBHcm91cDELMAkGA1UEBhMCSVIxFDASBgNVBAUTCzE0MDAzNzc40TkwMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAzLgyk5K06+j9d1ud0ilJArrZ3Whw/w9wEzHB9yXwENRa5fm5AbRukMF5b6VGeKzD6LZuL9+tfdFfWyPcjI++gGNywzRmEHKpTnzP1t6NyuXKfm4nBVAblsugSw8Y5DEXRfTqILgBWN/pZ4zGlifEALMcGAs7ADcjnv7b/tM2wxr9rHxsCvW4HvlzQasK8Qr1CrKgT0EI66rSXCHep/uIONDWp0W2OelMlZtM6AAjWXRLGcshPIHuK+ZLfAFxWtoGonf6qN9ypos2B18D/EFa8WHON62eYKT0kW3j

RC_TICS.IS_v1.4

بهمن ۱۴۰۳

سند « دستورالعمل فنی اتصال به سامانه مودیان »



BVa3yPEkRwkdDjDu/3CPzymhf3WFYwxpb4t35oWb/qUXGVIdvwIDAQABoy4wLDAf BgNVHSMEGDAWgBSx+Oq+RO3x/FmyCp+jcmfOH+Fn9TAJBgNVHRMEAjAAMA0GCSqG SIb3DQEBCwUAA4IBAQAgKATXlnS+pPtAiRIYGtydVU5Vi7Aq+D6QW07uFqcB7vBh ddN3yX2lVVcwpTNJzhv8UCM+mDMvlmsRVKVtMoo5fHfII92/Wo8rUz1RP+yhyCk0 Vz8I11v+bjLwVur/agC/s5Rf0m66pNNjFZ9J3S2N3lChXYwz2vvA8pdAYvWTu9g5 u4FMFqlsaLwMGC+WaA0g3KYzRkdWRy1vd23hLTUcVsWM8wpgZ11wEGE1khca/Sd0 mCU2HG5vIbqFfTjA6to0fY07CE5fD8aR3UcXjNduosV052ZqCX5SabrhFS3AGHFR jpFnI5LZespiCXSA8Sv3kOSCSRQKqFbiwSFM8Zjg

----END CERTIFICATE----

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

----BEGIN PRIVATE KEY----

MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDMuDKTko7r6P13 W53SKUkCutndaHD/D3ATMcH3JfAQ1Frl+bkBtG6QwXlvpUZ4rMPotm4v36190V9b I9yMj76AY3LDNGYQcqlOfM/W3o3K5cp+bicFUBuWy6BLDxjkMRdF9OoguAFY3+ln jMaWJ8QAsxwYCzsANyOe/tv+0zbDGv2sfGwK9bge+XNBqwrxCvUKsqBPQQjrqtJc Id6n+4g40NanRbY56UyVm0zoACNZdEsZyyE8ge4r5kt8AXFa2gaid/qo33KmizYH XwP8QVrxYc43rZ5gpPSRbeMFVrfI8SRHCR0OMO7/cI/PKaF/dYVjDGlvi3fmhZv+ pRcZUh2/AgMBAAECggEACPpC7YnNzram9ucDosXAt+ftyfHckrLgnVbfRLFbN8G4 QsGSxWpeNublJmo/Due0p63oYx0SBKR75AlMkLV1CzhRPhI8L5h3qEN88dVMrosp OCYoe+kpbJF9dA0zcD5e4Oh+o/StynH3UF0yED+qLsWsA7nqWnYQj9ZpW2Fz01Z1 i5NRX4YgyIopHfqcLWJWpOR8n4HwDY18BL7tMi31f0sZXz56EUgBPxq5RMi+1iKW pyZdwy4TrJL/Sj4tWkKJ7ELVd47VunizAgeLDy8bL1PBX0PewRvR37P9axHLjsj/ d1Iw/xvqgVEWZTyUXzg4qgFU5Na5u6xIW8JyqejdEQKBgQD2QlDdoPOtG1URyuuo 4HJlQ85ZfEWWA0vvp8esvJLJ7t73Rz28RkKAMHW/njr23ExxV3eek9J1lGENJUZF KsNNtjRWMgCxUicO0MGTJuraWHrEma00YNNjpVd3pIi68p51CZNzMRLn2J8F+7CP eGiynKEvKU43KcJr6KOkWP14FQKBgQDU0T3SNr7af4y3r03ds2DMaoKEG531tuLu nrZNnL4a/i2r3AlI5K470UkmAXDD1kgGf235KxrRm7x7VVp5SZLgOPqgJ2OKKk9b HLvuAdxCeUlnDfJWrAmYcmyLLCSDHBudN/evF6WiNaQi074MhdbaxYdLiiXdS3VV flQ/8m6/gwKBgD4ijXTeX52V/+j1YnDB8RtL+IzrpkMrocVeeCtFiWQaOXf7KcCP mcfuckdfDVGsVD1k7HG+qqOwRKykcw6Qs6awCpSVGUekiuZaFf2jHC7r1E522BUX OT8zQNaXVUiWXxT4zZOLF1IZfkZsMyiAISqwCptzuKCCkOPZVzDoo0vhAoGBAMo8 2XnVyoKLKWc2r4i600eo48S1FeP12yuVqXqR1FqEZ1RlMnGR1z1DAjdasRV5oVKD cDeTzdWZIIE3uFWAJFJt80WUiNQ4ptbXtINWQ0DsT2PebggNTsUPH7UVytDJ0jiq gfZjC2TdgtAR1g3Cdk3J3mtbqeXlGmiXN2rZcIMPAoGADfTonaehrsnscUcH4Dgs qZdyZm9JRmoNyisLBmbGkTNxoY09Vm/03u3NMsohkjopt2ly38ZMYX14FyXKEKcI 977r33JD9PxRcovqFhcPR3WuQrPf6ND3IX6eB5p8d7m6fmFYSe/0NhWoeH99a6/c csAr2hPMOb/R3GdRewkSGgQ=

----END PRIVATE KEY----