



نظام پایانه های فروشگاهی و سامانه مودیان

«دستور العمل فنی نحوه اتصال به سامانه مودیان»

(نحوه تبادل اطلاعات میان پایانه فروشگاهی - حافظه مالیاتی با سامانه مودیان)

شناسه سند: RC_TICS.IS_V01

خرداد ماه ۱۴۰۱

دولت کام
حسابداری
www.Hesabdary.Com
@HesabdaryCom

فهرست مطالب

۵	۱- مقدمه
۵	۲- هدف
۵	۳- دامنه کاربرد
۵	۴- تعاریف
۸	۵- پیکربندی پایانه فروشگاهی-حافظه مالیاتی
۸	۵-۱ دریافت شناسه یکتای حافظه مالیاتی
۹	۵-۲ پیکربندی و ثبت مشخصات
۹	۶- امنیت اطلاعات
۹	۶-۱ توکن
۱۰	۶-۲ امضا
۱۰	۶-۲-۱ نرمالسازی درخواست
۱۱	۶-۲-۲ فرآیند امضا صورتحساب
۱۴	۶-۳ نحوه رمزگذاری صورتحساب
۱۵	۷- فراخوانی متدهای API جمع آوری اطلاعات سامانه مودیان
۱۵	۷-۱ آدرس API ها
۱۶	۷-۲ ساختار درخواست ها
۲۰	۷-۳ سرویس های جمع آوری و پردازش اطلاعات
۲۰	۷-۳-۱ متد غیرهمگام
۲۰	۷-۳-۱-۱ سرویس درخواست غیرهمگام (ارسال صورتحساب)
۲۱	۷-۳-۱-۲ ساختار بسته صورتحساب
۲۶	۷-۳-۱-۳ پاسخ درخواست غیرهمگام
۲۷	۷-۳-۲ متدهای همگام
۲۷	۷-۳-۲-۱ سرویس درخواست های همگام
۲۹	۷-۳-۲-۲ پاسخ درخواست های همگام
۳۰	۷-۳-۲-۳ متد دریافت توکن
۳۰	۷-۳-۲-۴ متد استعلام اطلاعات حافظه مالیاتی مودی و حد مجاز فروش مودی

- ۳۰ ۵-۲-۳-۷ متدهای استعلام بسته‌های ارسالی غیر همگام
- ۳۱ ۶-۲-۳-۷ متد دریافت اطلاعات سرور
- ۳۱ ۷-۲-۳-۷ متد دریافت لیست کامل شناسه کالا/خدمات و نرخ مالیاتی
- ۳۲ ۸-۲-۳-۷ متد استعلام اطلاعات شماره اقتصادی
- ۳۲ ۸- لیست خطاها
- ۳۲ ۱-۸ مدل داده خطاها
- ۳۳ ۲-۸ لیست خطاهای لایه انتقال
- ۳۴ ۳-۸ لیست خطاهای لایه محتوا
- ۳۸ پیوست ۱
- ۵۵ پیوست ۲

فهرست شکل‌ها

- شکل ۱. نمودار آماده سازی صورتحساب جهت ارسال ۹
- شکل ۲. روش نرمالسازی درخواست ۱۰
- شکل ۳. نمودار ترتیبی فرآیند ارسال صورتحساب ۲۱

فهرست جداول

- جدول ۱. روش نرمالسازی JSON ۱۱
- جدول ۲. متدهای همگام و غیر همگام ۱۶
- جدول ۳. ساختار کلی درخواستها ۱۷
- جدول ۴. توضیحات مربوط به فیلدهای درخواست ۱۷
- جدول ۵. ساختار بسته (PACKET) ۱۸
- جدول ۶. توضیحات فیلدهای بسته (PACKET) ۱۹
- جدول ۷. اقلام صورتحساب ۲۱
- جدول ۸. مدل داده پاسخهای غیر همگام ۲۶
- جدول ۹. توضیحات فیلدهای خروجی درخواست غیر همگام ۲۶
- جدول ۱۰. درخواستهای همگام ۲۷
- جدول ۱۱. توضیحات فیلدهای ساختار خروجی درخواست همگام ۲۹
- جدول ۱۲. ساختار خروجی پاسخ خطا ۳۲
- جدول ۱۳. خطاهای لایه انتقال ۳۳
- جدول ۱۴. کدهای خطای دریافتی از هسته مالیاتی یا به عبارتی کدهای خطای لایه محتوا ۳۴

۱- مقدمه

در این سند نحوه اتصال به سامانه مودیان، دریافت اطلاعات مورد نیاز جهت پیکربندی پایانه فروشگاه‌های-حافظه مالیاتی، ارسال اطلاعات صورتحساب الکترونیکی و استعلام وضعیت صورتحساب‌های ارسالی شرح داده شده است. برای ارسال اطلاعات صورتحساب الکترونیکی از مکانیزم غیر همگام و برای دریافت و استعلام اطلاعات از مکانیزم همگام استفاده شده است. برای هر کدام از این مکانیزم‌ها، API مستقلی در نظر گرفته شده است. برای مکانیزم غیر همگام از صف استفاده می‌شود.

در کلیه مراحل استفاده از API، اصول امنیت اطلاعات شامل احراز هویت و سطح دسترسی ارسال‌کننده، محرمانگی، انکارناپذیری و یکپارچگی رعایت شده است.

۲- هدف

این سند با هدف تشریح نحوه اتصال به سامانه مودیان ارائه شده است. در این سند مراحل اتصال به سامانه مودیان شامل دریافت اطلاعات مورد نیاز جهت پیکربندی پایانه فروشگاه‌های-حافظه مالیاتی، ارسال اطلاعات صورتحساب الکترونیکی و استعلام وضعیت صورتحساب‌های ارسالی به صورت گام به گام و همراه با جزئیات فنی مورد نیاز برای پیاده‌سازی آن توسط کلیه ذی‌نفعان ارائه شده است.

۳- دامنه کاربرد

ذینفعان این سند شامل:

- اشخاص مشمول (مودیان).
- شرکت‌های معتمد ارائه‌کننده خدمات مالیاتی نوع اول



۴- تعاریف

- **شناسه یکتای حافظه مالیاتی:** شناسه‌ای است یکتا دارای مقداری ثابت و منحصر به فرد که به هر حافظه مالیاتی در سطح کشور اختصاص داده می‌شود، این شناسه از مولفه‌های تشکیل دهنده شماره

منحصر به فرد مالیاتی می باشد که پس از درخواست مودی در کارپوشه تولید و در اختیار وی قرار خواهد گرفت.

- **شماره منحصر به فرد مالیاتی:** شماره ای است یکتا در سامانه مودیان که به ازای هر صورتحساب تولید شده و به صورت منحصر به فرد به آن صورتحساب تخصیص داده می شود. این شماره دارای بخش های اطلاعاتی خاص بوده که جزئیات آن در سند «قالب شناسه یکتای حافظه مالیاتی و شماره منحصر به فرد مالیاتی» ذکر شده است.

- **صورتحساب الکترونیکی:** 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 الکترونیکی^۱، متناسب با نوع کسب و کار توسط سازمان تعیین و اعلام شده است. در مواردی که از دستگاه کارتخوان بانکی یا درگاه پرداخت الکترونیکی به عنوان پایانه فروشگاهی استفاده شود، رسید یا گزارش الکترونیکی پرداخت خرید صادره در حکم صورتحساب الکترونیکی است.

- **حافظه مالیاتی:** نوعی حافظه الکترونیکی است که برای ثبت و نگهداری اطلاعات مندرج در صورتحساب های الکترونیکی و انتقال آن به سامانه مودیان مورد استفاده قرار می گیرد. حافظه مالیاتی می تواند به شکل سخت افزاری یا نرم افزاری باشد. حافظه مالیاتی، توسط مودی برای ثبت صورتحساب الکترونیکی مورد استفاده قرار می گیرد. هر حافظه مالیاتی باید دارای شماره شناسه یکتا باشد. شناسه یکتای حافظه مالیاتی توسط سازمان اختصاص داده می شود.

- **پایانه فروشگاهی:** رایانه، دستگاه کارتخوان بانکی، درگاه پرداخت الکترونیکی یا هر وسیله دیگری که امکان اتصال به شبکه های الکترونیکی پرداخت رسمی کشور و سامانه مودیان را داشته و از قابلیت صدور صورتحساب الکترونیکی برخوردار باشد (بند ب ماده ۱ قانون).

- **شرکت های معتمد ارائه کننده خدمات مالیاتی:** اشخاص حقوقی دارای پروانه هستند که حسب ضوابط و دستورالعمل های ابلاغی سازمان، نسبت به ارائه مشاوره و آموزش های لازم به مودیان، نصب

^۱ مطابق سند دستورالعمل صدور صورتحساب الکترونیکی RC_IITP.IS_V03

و پشتیبانی تجهیزات مورد نیاز برای ارائه خدمات مالیاتی از قبیل خدمات مربوط به صدور صورتحساب و سایر امور غیرحاکمیتی با سازمان همکاری می کند (بند چ ماده ۱).

- **زیرسامانه جمع آوری و پردازش اطلاعات صورتحساب:** زیرسامانه ای است که داده های ارسالی از پایانه های فروشگاه - حافظه مالیاتی یا شرکت های معتمد ارائه کننده خدمات مالیاتی نوع اول را از طریق واسطه های نرم افزاری دریافت می کند.

- **حد مجاز فروش:** جمع صورتحساب های الکترونیکی صادره توسط هر مودی در هر دوره مالیاتی نمی تواند بیشتر از سه برابر فروش اظهار شده وی در دوره مشابه سال قبل، که مالیات آن به سازمان پرداخت شده یا ترتیب پرداخت آن داده شده است، باشد. جمع صورتحساب های الکترونیکی صادره شده در هر دوره مالیاتی برای واحدهای جدیدالتاسیس یا واحدهای فاقد سابقه مالیاتی نمی تواند بیش از سه برابر معافیت سالانه موضوع ماده (۱۰۱) قانون مالیات های مستقیم باشد (ماده ۶ قانون پایانه های فروشگاه و سامانه مودیان).

- **شناسه یکتای ارسال صورتحساب:** شناسه ای یکتا که هنگام ارسال صورتحساب توسط ارسال کننده به صورتحساب جهت رهگیری آن اختصاص داده می شود. این شناسه با فرمت ^۲uuid به صورت رمز نشده ارسال می گردد.

- **رسید یکتای دریافت صورتحساب:** هنگام دریافت صورتحساب در زیرسامانه جمع آوری و پردازش اطلاعات، یک شناسه رسید یکتا با فرمت ^۳uuid به هر صورتحساب توسط این زیرسامانه اختصاص داده می شود.

- **لیست صورتحساب ها:** مجموعه ای از صورتحساب های صادر شده توسط پایانه فروشگاه - حافظه مالیاتی که در قالب یک مجموعه به سامانه مودیان ارسال می شود.

- **کلاینت:** ارسال کننده درخواست به API زیرسامانه جمع آوری و پردازش اطلاعات که می تواند مودی یا شرکت معتمد ارائه کننده خدمات مالیاتی باشد.

- **سرور:** سرور سامانه مودیان

2 uid

3 Universal unique identificatier

4 reference_number

- **زوج کلید عمومی و خصوصی:** در این سند هر گاه برای انکار ناپذیری از کلید عمومی یا خصوصی استفاده می شود منظور کلیدی است که توسط یک مرکز میانی معتبر برای هر یک از ذینفعان سامانه مودیان گواهی شده باشد.

- **مرکز میانی معتبر:** هر مرکز میانی که از شورای سیاست گذاری گواهی الکترونیکی کشور مجوز گرفته باشد (موضوع ماده ۳۲ قانون تجارت الکترونیکی). لیست این مراکز از طریق سایت www.rca.gov.ir بخش مراکز میانی، قابل دسترسی است.



۵- پیکربندی پایانه فروشگاه - حافظه مالیاتی

۵-۱ دریافت شناسه یکتای حافظه مالیاتی

مودی جهت صدور و ارسال صورتحساب الکترونیکی نیاز به دریافت شناسه یکتا حافظه مالیاتی دارد. بنابراین می بایست 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 خود مودی (به روش مستقیم)
- ارسال اطلاعات صورتحساب توسط شرکت معتمد ارائه کننده خدمات مالیاتی (به روش غیرمستقیم)
- ارسال اطلاعات صورتحساب توسط شرکت معتمد ارائه کننده خدمات مالیاتی (به روش غیرمستقیم و با استفاده از زیرساخت های اختصاصی)

۲. کلید عمومی (RSA) دریافتی از مراکز میانی معتبر با طول کلید ۲۰۴۸ بیت را بارگذاری نماید.

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 توسط مودی ضرورتی ندارد. در این حالت شرکت معتمد ارائه کننده خدمات مالیاتی باید از طریق کارپوشه خود،

کلید عمومی مربوطه را به سازمان معرفی نماید.

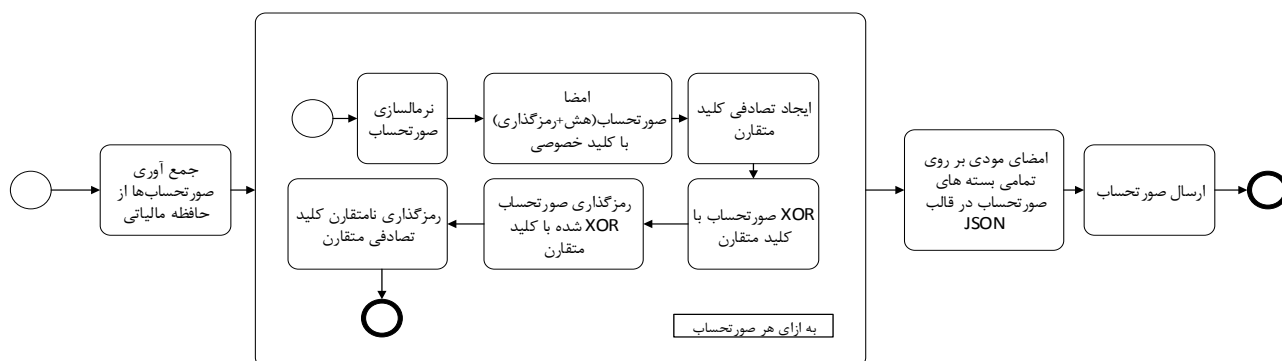
۳. ارتباط شناسه یکتای حافظه مالیاتی درخواستی با کدپستی (های) محل فعالیت تعیین گردد.

۵-۲ پیکربندی و ثبت مشخصات

مودی برای راه اندازی پایانه فروشگاهی-حافظه مالیاتی خود باید از طریق فراخوانی متدهای "دریافت اطلاعات سرور" و "دریافت اطلاعات حافظه مالیاتی"، شماره اقتصادی، نام تجاری، ساعت و تاریخ، کلید عمومی سازمان و شناسه یکتای حافظه مالیاتی را از سرور دریافت کند. جزئیات اقلام اطلاعاتی لازم در جدول ۱۰ توضیح داده شده است.

۶- امنیت اطلاعات

مکانیزم‌های امنیتی جهت ارسال صورتحساب مطابق با نمودار ارائه شده در شکل (۱) می‌باشند.



شکل ۱. نمودار آماده سازی صورتحساب جهت ارسال

۶-۱ توکن

با هدف احراز هویت و تعیین سطح دسترسی ارسال کننده اطلاعات، از مکانیزم تخصیص توکن JWT^۵ استفاده شده است. لازم است توکن تخصیص داده شده به مودی یا شرکت معتمد ارائه کننده خدمات مالیاتی نوع اول در Header تمامی درخواست‌های ارسال شده مودی به API های زیرسامانه جمع آوری و پردازش اطلاعات قرار گیرد.

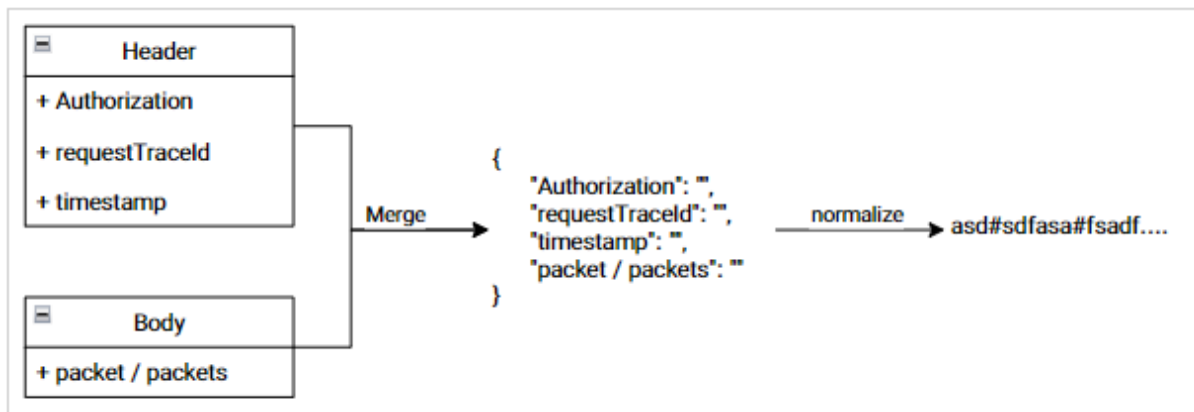
^۵ Json Web Token

۶-۲ امضا

با هدف حفظ قابلیت انکارناپذیری، یکپارچگی و احراز هویت، بر روی تمامی درخواست‌ها به API های زیرسامانه جمع آوری و پردازش اطلاعات مکانیزم امضا در نظر گرفته شده است.

۶-۲-۱ نرمالسازی درخواست

برای یکسان کردن ساختار تمامی درخواست‌ها به API های زیرسامانه جمع آوری اطلاعات، برای تمامی بسته‌های ارسالی شامل همگام و غیرهمگام امضا بر روی درخواست صورت می‌پذیرد. برای امضا می‌بایست ابتدا Header و Body درخواست ادغام و JSON واحد تولید گردد. ضروری است JSON تولید شده مطابق شکل (۲) به رشته تبدیل، سپس امضا و ارسال شود.



شکل ۲. روش نرمالسازی درخواست

فرآیند تبدیل JSON به رشته، مطابق گام‌های جدول (۱) می‌باشد:

- شی به فرمت کلید-مقدار تبدیل شده به طوری که کلید، عمق جایگاه مقدار را مشخص می‌نماید.
- کلیدها بر اساس حروف الفبا مرتب شوند.
- سپس مقادارها به ترتیب با هم ادغام شوند:
- از کاراکتر # به عنوان جداکننده مقادیر (اقلام اطلاعاتی) استفاده شود.
- در صورتی که کاراکتر # در متن وجود داشته باشد، با ## مشخص می‌گردد.
- در صورتی که مقدار فیلدی در رشته، null یا "" باشد؛ با ### مشخص می‌گردد.
- در آخر آرایه‌ای از روی این رشته ایجاد می‌شود.

جدول ۱. روش نرمالسازی JSON

گام ۱	<pre>{ "k2": "v1", "k4": "v2", "k3": { "k1": "v4", "k5": "v5" } }</pre>	 <pre>"k2": "v1" "k4": "v2" "k3.k1": "v4" "k3.K5": "v5"</pre>
گام ۲	<pre>"k2": "v1" "k3.k1": "v4" "k3.K5": "v5" "k4": "v2"</pre>	
گام ۳	v1#v4#v5#v2	

نکات:

- در صورتی که داخل JSON آرایه وجود داشته باشد، ترتیب عناصر آرایه دست کاری نشده و با همان ترتیب در نظر گرفته می شود.

- در صورتی که ریشه JSON آرایه باشد، داخل فیلد packets قرار گرفته و تبدیل به شی می شود.

روش پیاده سازی نرمالسازی JSON در پیوست های ۱-۱ و ۱-۲ ارائه شده است.

۶-۲-۲ فرآیند امضا صورتحساب

برای امضا صورتحساب باید اطلاعات JSON صورتحساب به روشی که برای نرمال سازی بیان شد نرمال

شوند. به عنوان مثال اطلاعات JSON صورتحساب زیر را در نظر بگیرید:

```
{
  "header" :
  {
    "taxid": "AA56CD0E062002F2B4E78",
    "indatim": "1655620821274",
    "indati2m": "1655620821274",
    "inty": 2,
    "inno" : "0002F2B4E7",
    "irtaxid" : null,
    "inp": 1,

```

```
"ins" : 1,
"tins" : "32652362589632",
"tob" : 1,
"bid" : null,
"tinb" : null,
"sbcb" : null,
"bpc" : null,
"bbc" : null,
"ft" : null,
"bpn" : null,
"scln" : null,
"scc" : null,
"crn" : null,
"billid" : null,
"tprdis" : 1000000,
"tdis" : 0,
"tadis" : 1000000,
"tvam" : 90000,
"todam" : 0,
"tbill" : 1090000,
"setm" : 1,
"cap" : 90000,
"insp" : 0,
"tvop" : 90000,
"dpvb" : null,
"tax17" : null
}
"body" : [
{
"sstid" : 2153265989636,
"sstt" : "پاستیل میوه ای شیبابا",
"mu" : 96,
"am" : 1,
"fee" : 1000000,
"cfee" : null,
"cut" : null,
"exr" : null,
"prdis" : 1000000,
"dis" : 0,
"adis" : 1000000,
"vra" : 0.09,
"vam" : 90000,
"odt" : null,
"odr" : null,
"odam" : null,
```

```

    "olt" : null,
    "olr" : null,
    "olam" : null,
    "consfee" : null,
    "spro" : null,
    "bro" : null,
    "tcpbs" : null,
    "cop" : 90000,
    "vop" : 90000,
    "bsrn" : null,
    "tsstam" : 1090000
  }
],
"payments" : [
  {
    "iinn" : 5646556,
    "acn" : 5656565,
    "trmn" : 54554224,
    "trn" : 544542424,
    "pcn" : "6037-9972-9856-9865",
    "pid" : null,
    "pdt" : 1655620821274,
  }
],
"extension": [
  {
    "key" : null,
    "value" : null
  }
]
]
}

```

❖ تمام اطلاعات پر شده در JSON غیر واقعی و تستی می باشد.

بعد از نرمال سازی JSON صورت حساب مورد نظر، رشته نرمال شده به صورت زیر بدست می آید:

1000000#1#####90000###0###1000000#96#####1000000###2153265
 989636# پاستیل میوه ای
 ۱#۱۶۵۵۶۲۰۸۲۱۲۷۴#####۹۰۰۰۰#####۰,۰۹#۹۰۰۰۰#۹۰۰۰۰#۱۰۹۰۰۰۰#####شیبایا
 ۶۵۵۶۲۰۸۲۱۲۷۴#۰۰۰۲F2B4E7#1#1#0.0#2#####1#1000000###AA56CD0E0620002F2
 B4E78#1090000#0###32652362589632#1#0.0#1000000#90000#90000#5656565#5646556
 #6037 - 9972 - 9856 - 9865#1655620821274#null#54554224#544542424

رشته تولید شده در مراحل بالا به وسیله کلید خصوصی (مودی/شرکت معتمد) با الگوریتم RSA2048-

SHA256 هش و امضا می‌شود و خروجی آن در فیلد dataSignature در شی packet قرار می‌گیرد.

❖ کد روش امضا در پیوست شماره ۱-۳ ارائه شده است.

۳-۶ نحوه رمز گذاری صورتحساب

برای رمز گذاری صورتحساب می‌بایست یک کلید متقارن (به روش AES/GCM/NoPadding) با طول ۲۵۶ بیت تولید شود. برای رمز گذاری از طریق AES/GCM نیاز به یک کلید دیگر به نام IV به طول ۱۲۸ بیت می‌باشد که این کلید به صورت تصادفی تولید می‌گردد. بعد از تولید کلیدهای مورد نیاز، JSON صورتحساب را ابتدا با کلید متقارن XOR کرده و سپس به روش AES/GCM رمز گذاری می‌گردد.

جزئیات XOR به این شکل است که باید متنی که می‌خواهیم XOR کنیم (در اینجا JSON صورتحساب) باید به بلاک های ۲۵۶ بیتی تبدیل شود و هر بلاک با کلید متقارن که ۲۵۶ بیت است XOR شود. با این روش ممکن است که بلاک آخر تعداد بیت کمتر از ۲۵۶ داشته باشد که با همان تعداد از کلید متقارن XOR انجام می‌شود.

برای صورتحساب تستی بخش قبل کلید متقارن رمز شده و IV به صورت hex در زیر نمایش داده شده است :

AES key : 4fda3c622e966e0839441401bbd3b8f191d4267bf5f19b40812a34b212fd3ed9

IV : 4fda3c622e966e0839441401bbd3b8f191d4267bf5f19b40812a34b212fd3ed9

نمونه صورتحساب رمز شده به شکل زیر است :

```

rvd4iGRTYa68VppDwli9cGf+d0Qfo6g9Eu4hsyqQe4vwY17F2dQvXgvK6KwDJR2
RQIdhXcx6SM+UF/XE4CJxMgmjFMvBBjM34ix2ZFIaR2v2rwZ6XLUPTHWK
HIXROxnA10BagrgOm0Xr4J6Y359ZZpnaNChPabj7s4yE4ZGT+wBHoz+J/yj2xFW
KWmmcuP1b6rWodWYO2OD6eXI1+faxT2vZ7FSBYyDy+sJP5S6Zllp92baFHX7
Z78VVqVGv+P+iJ+CLljD6j75k19ykD7stVkvHsoMwWYndqNiBIRLBXOjczSkJ/y
L89eiGKcAUvEAGSiXgaeKjEymLaOWXZEdg0IwxVUrgRyX+4kVbWeCUWHSb
jafCdQNRUddFZLWs3bO6MA552gaAh9iXJGmnJNvCbWjppjTvx9NyDbvd3thZhFl
dhX5dkVEi7mWv3iTywRCUN/6QkOxZ4JDG7u3i20vqztuqxq/Kj/51GMOGov2hhF
jd+5c6QckvO7COMX4XVO6azrWGa3VVyZz6dG9vCvVb/BZsVTxGBddQiQKd5
aaQxxIvs+sM7/FibQ415lISN+4ax8g420qO5E6hA+mMQ3oECnJtyKJmDK6oR6T5y
//5dBjFffMySmhdx+bhS0XxMFvk7ZPUcWFZwDGS6yNKA2AApt58xqGnbuf+N2
86UjPH9CgNogY/G5lvFIPX51qi6q6X/YX165WhD0MbVEL8EEyfk/60rjwLivhEkc
ZWowhyOBnxtHvVmpjocTS/404Oskepra/4jRKiqON3hqwpEJE8V0hanYwp9m32
HtYbiql9RqL3wHycbWtnueFNjptlKi4tcz14NsfD9ezD6TQVgcAT0o14OAnklJTO/
0QnwfTgv8krEy7F/umNYWPswgWrjqSHtGiUHbXLunGP6fwZZOT0vECwXrz9X/

```

aHGX/rm64/orJArZ9Vi2OIdzvGdQbcXsGAKKuAICvssA4XnXMBvWW9+g4Y+q
 qsHBTomkvHYrXvLob02FUWL0XsTkap/BXfLlj4HBQUhh0gUk6aX8wetRknFiH
 HjblgjN7Tjc51Jt1GifTZhNg/uHIJB/6/GlwIbxAPXB4YfNiRAU0y0iCiU1Ow8Jl6Tu
 us3cgGkLvo5uOIF/0vLx9O2BSJHcpA0OBhIjaJ1bdgHSYOr3P3tDY+BVSe33/8oO
 0DAVBjEDUQKx3F0Ncr6TwxlqewquIHL2zmktSMc2KbIFY12Jx7cG84hh4Ih98Vi
 Fg+Xad83Ed3G/JiU3uG+7qiaYi8DYI6Icw0rf870qQ/CkopVR44xRtePsIZfZjKS0X5
 39/4qymPDs3+KFYZGntliwc6fRNSLhjoTidCHFRcF9tP2Ttkp6CTsnLsHtQugYZatn
 rMO+X+GNxihIF9Be9/UJMdJ9vzwLWUn+/0+ducZKJ3mpTw5T8DqYuhzOcpYoR
 obear9uzYb+2Ky8g==

کد روش رمزگذاری به روش متقارن AES/GCM در پیوست ۱-۴ ارائه شده است.

پس از رمزگذاری صورتحساب، از طریق الگوریتم AES/GCM، باید کلید متقارن رمز شده و IV در کنار صورتحساب رمز شده قرار گیرد. برای رمزگذاری کلید متقارن باید از روش نامتقارن RSA-OAEP-SHA256 استفاده شود که برای این منظور از کلید/های عمومی سازمان با طول ۴۰۹۶ بیت اخذ شده از یک مرکز میانی معتبر استفاده می شود (کلید عمومی سازمان با استفاده از متد GET_SERVER_INFORMATION به دست می آید).

کد روش رمزگذاری به روش نامتقارن RSA-OAEP-SHA256 در پیوست ۱-۵ ارائه شده است.

۷- فراخوانی متدهای API جمع آوری اطلاعات سامانه مودیان

۷-۱ آدرس API ها

آدرس API های زیرسامانه جمع آوری و پردازش اطلاعات به صورت زیر است که پیشوند تمام آدرسها قرار می گیرد.

<https://tp.tax.gov.ir/req/>

آدرس هایی که با tsp شروع می شوند برای شرکت های معتمد ارائه کننده خدمات مالیاتی در نظر گرفته شده و آدرس هایی که با self-tsp شروع می شوند برای مودیانی که قصد دارند خودشان صورتحساب ارسال کنند در نظر گرفته شده است.

دو مکانیزم برای درخواست‌های با اولویت عادی و درخواست‌های با اولویت بالا وجود دارد. آدرس normal-enqueue برای درخواست‌های معمولی و fast-enqueue برای درخواست‌های با اولویت بالا در نظر گرفته شده است.



www.Hesabdar.com
@HesabdarCom

متدها همراه با آدرس API در جدول (۲) ارائه شده اند.

جدول ۲. متدهای همگام و غیرهمگام

آدرس متد	اسم متد	ردیف
.../api/self-tsp/async/normal-enqueue/ .../api/self-tsp/async/fast-enqueue/ .../api/tsp/async/normal-enqueue/ .../api/tsp/async/fast-enqueue/	ارسال صورتحساب الکترونیکی	۱
.../api/self-tsp/sync/ GET_TOKEN/ .../api/tsp/sync/ GET_TOKEN/	متد دریافت توکن	۲
.../api/self-tsp/sync/ GET_FISCAL_INFORMATION/ .../api/tsp/sync/ GET_FISCAL_INFORMATION/	استعلام اطلاعات حافظه مالیاتی مودی و حد مجاز فروش مودی	۳
.../api/self-tsp/sync/ INQUIRY_BY_UID / .../api/tsp/sync/ INQUIRY_BY_UID /	استعلام با شناسه یکتای ارسال صورتحساب	۴
.../api/self-tsp/sync/INQUIRY_BY_REFERENCE_NUMBER / .../api/tsp/sync/INQUIRY_BY_REFERENCE_NUMBER /	استعلام با رسید یکتای دریافت صورتحساب	۵
.../api/self-tsp/sync/INQUIRY_BY_TIME/ .../api/tsp/sync/INQUIRY_BY_TIME /	دریافت خطاهای بسته‌های ارسالی غیرهمگام با استفاده از زمان	۶
.../api/self-tsp/sync/ INQUIRY_BY_TIME_RANGE / .../api/tsp/sync/ INQUIRY_BY_TIME_RANGE /	دریافت خطاهای بسته‌های ارسالی غیرهمگام با استفاده از بازه زمانی	۷
.../api/self-tsp/sync/ GET_SERVER_INFORMATION / .../api/tsp/sync/ GET_SERVER_INFORMATION /	دریافت اطلاعات سرور	۸
.../api/self-tsp/sync/ GET_SERVICE_STUFF_LIST / .../api/tsp/sync/ GET_SERVICE_STUFF_LIST /	دریافت لیست کامل شناسه کالا/خدمات و نرخ مالیاتی	۹
.../api/self-tsp/sync/GET_ECONOMIC_CODE_INFORMATION / .../api/tsp/sync/GET_ECONOMIC_CODE_INFORMATION /	استعلام اطلاعات شماره اقتصادی	۱۰

۷-۲ ساختار درخواست‌ها

در این بخش ساختار درخواست‌ها به API شرح داده شده است. در جدول (۳) ساختار کلی درخواست ارائه شده است.

ساختار کلی سرویس همگام مشابه با سرویس غیر همگام بوده و تفاوت آن در فیلد packet است. بطوریکه در حالت همگام به جای آرایه‌ای از درخواست، فقط یک درخواست می‌توان ارسال نمود (packet). در درخواست غیر همگام می‌توان مجموعه‌ای از بسته‌ها (packets) را ارسال نمود.

جدول ۳. ساختار کلی درخواستها

عنوان	مقدار
متد HTTP	POST
فیلدهای Header	Authorization: "string" requestTraceId: "string" timestamp: "Long"
فیلدهای Body	<pre>{ "packets": Packet[], "signature": "string", "signatureKeyId": "string" }</pre>
فیلدهای خروجی	<pre>{ "timestamp": "Long", "result": AsyncResponse[], "signature": "string", "signatureKeyId": "string" }</pre>
خروجی سرویس در صورت رخداد خطای کلی	<pre>{ "timestamp": "Long", "errors": ErrorResponse[], "signature": "string", "signatureKeyId": "string" }</pre>

❖ فیلد signatureKeyId اختیاری بوده و مقدار پیش فرض آن برابر با null خواهد بود.

اطلاعات تکمیلی فیلدها در جدول (۴) آورده شده است:

جدول ۴. توضیحات مربوط به فیلدهای درخواست

نام فیلد	توضیحات
Authorization	توکن با این سرآیند (Header) ارسال می‌شود، در صورتیکه فراخوانی یک متد نیاز به احراز هویت نداشته باشد، این فیلد اختیاری خواهد شد. این سرآیند در API های غیر همگام و برخی از API

نام فیلد	توضیحات
	های همگام اجباری است.
requestTraceId	هر درخواستی باید دارای یک UUID باشد که در سرآیند ارسال می‌شود. از این شناسه برای تشخیص درخواست‌های تکراری استفاده می‌شود.
timestamp	زمان ارسال بسته از کلاینت که در سرآیند ارسال می‌شود. یکی از کاربردهای این فیلد، رد کردن بسته‌های قدیمی است.
packets	لیست بسته‌های ارسالی.
signature	امضای روی درخواست.
signatureKeyId	شناسه کلید عمومی ارسال کننده، برای بررسی امضا. این فیلد اختیاری بوده و مقدار پیش فرض آن برابر با Null خواهد بود.

زمانی که کلاینت پاسخ این سرویس را دریافت می‌کند، الزاماً رسیدگی به بسته‌های اطلاعاتی پایان نیافته است، بلکه تنها در صف رسیدگی قرار گرفته‌اند. تایید رسیدگی و نتیجه اعمال موفق یا ناموفق بسته‌های اطلاعاتی از طریق استعلام به اطلاع کلاینت خواهد رسید.

در صورتی که کلاینت، نتیجه رسیدگی به یک بسته را failed دریافت نماید، لازم است پس از اطمینان از عدم وجود خطاها در بسته ارسالی آن را مجدداً ارسال نماید. در ارسال مجدد باید مقدار فیلد retry برابر true باشد تا سرویس غیرهمگام در جریان ارسال مجدد درخواست باشد.

ساختار بسته‌های ارسالی به سرور و فیلدهای مربوطه به ترتیب مطابق جداول (۵) و (۶) می‌باشد.

جدول ۵. ساختار بسته (packet)

اسم شی	Packet
--------	--------

<pre>{ "uid": "string", "packetType": "string", "retry": "Boolean", "data": "string", "encryptionKeyId": "string", "symmetrickey": "string", "iv": "string", "fiscalId": "string", "dataSignature": "string" }</pre>	نوع فیلدها
--	------------

جدول ۶. توضیحات فیلدهای بسته (packet)

نام فیلد	توضیحات
uid	شناسه یکتای ارسال صورتحساب، کدی که در سمت کلاینت هنگام ارسال تولید می شود.
packetType	نوع بسته
retry	نوع فیلد بولین است (مقدار TRUE/FALSE)، مشخص می کند که بسته اولین بار است ارسال شده است یا خیر.
data	داده های داخل درخواست. در صورتی که داده ها رمز شده باشند، آرایه بایت به صورت رشته Base64 ارسال می شود. در صورتی که داده ها کشف باشند، رشته سریال شده JSON قرار داده می شود.
encryptionKeyId	شناسه کلید عمومی سازمان، جهت باز کردن کلید متقارن. در صورتی که داده ها رمز نشده باشند، این فیلد خالی ارسال می شود.
symmetrickey	کلید متقارن رمز شده با کلید رمزنگاری (کلید عمومی سازمان) جهت باز کردن داده های رمز شده. در صورتی که داده ها رمز نشده باشند، این فیلد خالی ارسال می شود.
iv	بردار مقدار اولیه کلید متقارن. در صورتی که داده ها رمز نشده باشند، این فیلد خالی ارسال می شود.
fiscalId	شناسه یکتای حافظه مالیاتی. در صورتی که ارسال کننده شرکت ارائه کننده خدمات مالیاتی باشد، این فیلد اجباری خواهد بود.
dataSignature	امضای صورتحساب.

۷-۳ سرویس های جمع آوری و پردازش اطلاعات

درخواست همگام و غیر همگام دو سرویس اصلی زیر سامانه جمع آوری و پردازش اطلاعات می باشند:

۷-۳-۱ متد غیر همگام

۷-۳-۱-۱ سرویس درخواست غیر همگام (ارسال صورتحساب)

ارسال صورتحساب به صورت غیر همگام انجام می شود و جهت ارسال به احراز هویت و امضا دیجیتال صورتحساب و کل لیست ارسالی و همچنین رمز گذاری نیاز است.

برای اینکه ساختار مناسبی برای رهگیری تغییرات بسته ها وجود داشته باشد، نوع بسته (PacketType) در صورتحساب به دو بخش تقسیم بندی می شود.

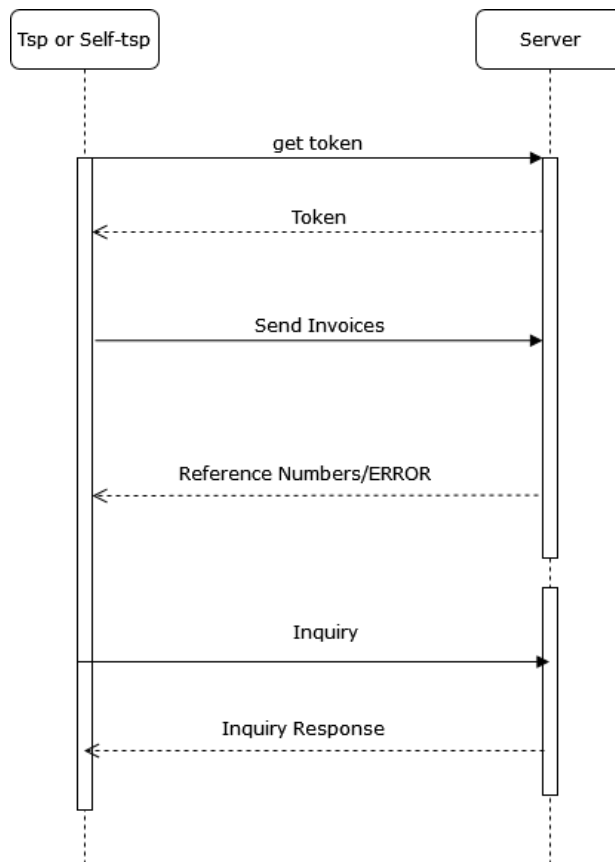
بخش اول	بخش دوم
INVOICE	شماره نسخه + حرف V

برای مثال اگر صورتحسابی با نسخه بسته 01 داشته باشیم، نوع بسته به صورت زیر خواهد بود:

INVOICE.V01

فرآیند ارسال صورتحساب مطابق شکل (۳) و به شرح ذیل می باشد:

۱. مودی یا TSP با ارسال درخواست توکن به سرور جمع آوری فرآیند ارسال صورتحساب را شروع می کند.
۲. توکن دریافت شده در سرآیند درخواست قرار می گیرد و صورتحساب ارسال می شود.
۳. مودی یا TSP رسید یکتای دریافت صورتحساب درخواست خود را از سامانه مودیان دریافت می کند.
۴. مودی یا TSP می تواند به وسیله فراخوانی متدهای اعلام از وضعیت ارسال صورتحساب خود با خبر شود.



شکل ۳. نمودار ترتیبی فرآیند ارسال صورتحساب

در صورتی که وضعیت درخواست به صورت "PENDING" باشد به این معنی است که هنوز درخواست پردازش نشده است.

نمونه CURL درخواست در پیوست ۲-۱ ارائه شده است.

۲-۱-۳-۷ ساختار بسته صورتحساب

شناسنامه همه اقلام اطلاعاتی که در انواع و الگوهای صورتحساب وجود دارند به شرح جدول (۷) می باشد:

جدول ۷. اقلام صورتحساب

ردیف	عنوان قلم اطلاعاتی	JSON	محل قرارگیری در صورتحساب	نوع فیلد	طول فیلد	مقادیر مجاز
۱	شماره منحصر به فرد مالیاتی	taxid	سرآمد (Header)	string	۲۲	
۲	تاریخ و زمان صدور صورتحساب (میلادی)	indatim	سرآمد (Header)	Timestamp	۱۴	

ردیف	عنوان قلم اطلاعاتی	JSON	محل قرارگیری در صورت حساب	نوع فیلد	طول فیلد	مقادیر مجاز
۳	تاریخ و زمان ایجاد صورت حساب (میلادی)	Indati2m	سرآمد (Header)	Timestamp	۱۴	
۴	نوع صورت حساب	inty	سرآمد (Header)	int	۱	۱- نوع اول ۲- نوع دوم ۳- نوع سوم
۵	سریال صورت حساب	inno	سرآمد (Header)	string	۱۰	
۶	شماره منحصر به فرد مالیاتی صورت حساب مرجع	irtaxid	سرآمد (Header)	string	۲۲	
۷	الگوی صورت حساب	inp	سرآمد (Header)	int	۱	۱- الگوی ۱: فروش ۲- الگوی ۲: فروش ارزی ۳- الگوی ۳: صورت حساب طلا، جواهر و پلاتین ۴- الگوی ۴: قرارداد پیمانکاری ۵- الگوی ۵: قبوض خدماتی ۶- الگوی ۶: بلیت هواپیما
۸	موضوع صورت حساب	ins	سرآمد (Header)	int	۱	۱- اصلی ۲- اصلاحی ۳- ابطالی ۴- برگشت از فروش

ردیف	عنوان قلم اطلاعاتی	JSON	محل قرار گیری در صورت حساب	نوع فیلد	طول فیلد	مقادیر مجاز
۹	شماره اقتصادی فروشنده	tins	سرآمد (Header)	int	۱۰	
۱۰	نوع شخص خریدار	tob	سرآمد (Header)	int	۱	۱-۲-۳-۴-۵ ۱- حقیقی ۲- حقوقی ۳- مشارکت مدنی ۴- اتباع غیر ایرانی ۵- مصرف کننده نهایی
۱۱	شماره/شناسه ملی/شناسه مشارکت مدنی/کد فراگیر خریدار	bid	سرآمد (Header)	int	متغیر	
۱۲	شماره اقتصادی خریدار	tinb	سرآمد (Header)	int	۱۰	
۱۳	کد شعبه فروشنده	sbc	سرآمد (Header)	int	متغیر	
۱۴	کد پستی خریدار	bpc	سرآمد (Header)	int	۱۰	
۱۵	کد شعبه خریدار	bbc	سرآمد (Header)	int	متغیر	
۱۶	نوع پرواز	ft	سرآمد (Header)	int	۱	۱- داخلی ۲- خارجی
۱۷	شماره گذرنامه خریدار	bpn	سرآمد (Header)	string	متغیر	
۱۸	شماره پروانه گمرکی فروشنده	scln	سرآمد (Header)	int	متغیر	
۱۹	کد گمرک محل اظهار	scc	سرآمد (Header)	int	متغیر	
۲۰	شناسه یکتای ثبت قرارداد فروشنده	crn	سرآمد (Header)	int	متغیر	
۲۱	شماره اشتراک/شناسه بهره بردار قبض	billid	سرآمد (Header)	int	متغیر	
۲۲	مجموع مبلغ قبل از کسر تخفیف	tprdis	سرآمد (Header)	double	متغیر	
۲۳	مجموع تخفیفات	tdis	سرآمد (Header)	double	متغیر	

ردیف	عنوان قلم اطلاعاتی	JSON	محل قرارگیری در صورت حساب	نوع فیلد	طول فیلد	مقادیر مجاز
۲۴	مجموع مبلغ پس از کسر تخفیف	tadis	سرآمد (Header)	double	متغیر	
۲۵	مجموع مالیات بر ارزش افزوده	tvam	سرآمد (Header)	double	متغیر	
۲۶	مجموع سایر مالیات، عوارض و وجوه قانونی	todam	سرآمد (Header)	double	متغیر	
۲۷	مجموع صورتحساب	tbill	سرآمد (Header)	double	متغیر	
۲۸	روش تسویه	setm	سرآمد (Header)	int	۱	۱-۲-۳ ۱- نقد ۲- نسیه ۳- نقد/نسیه
۲۹	مبلغ پرداختی نقدی	cap	سرآمد (Header)	double	متغیر	
۳۰	مبلغ پرداختی نسیه	insp	سرآمد (Header)	double	متغیر	
۳۱	مجموع سهم مالیات بر ارزش افزوده از پرداخت	tvop	سرآمد (Header)	double	متغیر	
۳۲	عدم پرداخت مالیات بر ارزش افزوده خریدار	dpvb	سرآمد (Header)	int	۱	۱- عدم پرداخت ۲- پرداخت
۳۳	مالیات موضوع ماده ۱۷	Tax17	سرآمد (Header)	double	متغیر	
۳۴	شناسه کالا/خدمت	sstid	بدنه (Body)	int	۱۳	
۳۵	شرح کالا/خدمت	sstt	بدنه (Body)	string	متغیر	
۳۶	واحد اندازه گیری	mu	بدنه (Body)	int	۳	از جدول پیوست ۸ دستورالعمل صدور صورتحساب الکترونیکی
۳۷	تعداد/مقدار	am	بدنه (Body)	int	متغیر	
۳۸	مبلغ واحد	fee	بدنه (Body)	double	متغیر	
۳۹	میزان ارز	cfee	بدنه (Body)	double	متغیر	
۴۰	نوع ارز	cut	بدنه (Body)	string	متغیر	
۴۱	نرخ برابری ارز با ریال	exr	بدنه (Body)	double	متغیر	
۴۲	مبلغ قبل از تخفیف	prdis	بدنه (Body)	double	متغیر	
۴۳	مبلغ تخفیف	dis	بدنه (Body)	double	متغیر	
۴۴	مبلغ بعد از تخفیف	adis	بدنه (Body)	double	متغیر	

ردیف	عنوان قلم اطلاعاتی	JSON	محل قرارگیری در صورت حساب	نوع فیلد	طول فیلد	مقادیر مجاز
۴۵	نرخ مالیات بر ارزش افزوده	vra	بدنه (Body)	double	متغیر	
۴۶	مبلغ مالیات بر ارزش افزوده	vam	بدنه (Body)	double	متغیر	
۴۷	موضوع سایر مالیات و عوارض	odt	بدنه (Body)	string	متغیر	
۴۸	نرخ سایر مالیات و عوارض	odr	بدنه (Body)	double	متغیر	
۴۹	مبلغ سایر مالیات و عوارض	odam	بدنه (Body)	double	متغیر	
۵۰	موضوع سایر وجوه قانونی	olt	بدنه (Body)	string	متغیر	
۵۱	نرخ سایر وجوه قانونی	olr	بدنه (Body)	double	متغیر	
۵۲	مبلغ سایر وجوه قانونی	olam	بدنه (Body)	double	متغیر	
۵۳	اجرت ساخت	consfee	بدنه (Body)	double	متغیر	
۵۴	سود فروشنده	spro	بدنه (Body)	double	متغیر	
۵۵	حق العمل	bro	بدنه (Body)	double	متغیر	
۵۶	جمع کل اجرت، حق- العمل و سود	tcpbs	بدنه (Body)	double	متغیر	
۵۷	سهم نقدی از پرداخت	cop	بدنه (Body)	double	متغیر	
۵۸	سهم ارزش افزوده از پرداخت	vop	بدنه (Body)	double	متغیر	
۵۹	شناسه یکتای ثبت قرارداد حق العملکاری	bsrn	بدنه (Body)	int	متغیر	
۶۰	مبلغ کل کالا/خدمت	tsstam	بدنه (Body)	double	متغیر	
۶۱	شماره سوییچ پرداخت	iinn	اطلاعات پرداخت (Payment)	int	متغیر	
۶۲	شماره پذیرنده فروشگاه	acn	اطلاعات پرداخت (Payment)	int	متغیر	
۶۳	شماره پایانه	trmn	اطلاعات پرداخت (Payment)	int	متغیر	
۶۴	شماره پیگیری	trn	اطلاعات پرداخت (Payment)	int	متغیر	

ردیف	عنوان قلم اطلاعاتی	JSON	محل قرارگیری در صورت حساب	نوع فیلد	طول فیلد	مقادیر مجاز
۶۵	شماره کارت پرداخت کننده صورت حساب	pcn	(Payment) اطلاعات پرداخت)	int	متغیر	
۶۶	شماره/شناسه ملی/کد فراگیر اتباع غیر ایرانی پرداخت کننده صورت حساب	pid	(Payment) اطلاعات پرداخت)	int	متغیر	
۶۷	تاریخ و زمان پرداخت صورت حساب	pdt	(Payment) اطلاعات پرداخت)	Timestamp	۱۴	

نکته قابل توجه در ارسال اطلاعات صورت حساب این است که در صورتی که پارامتری فاقد مقدار باشد، باید به صورت پیشفرض با مقدار null ارسال شود یا کلا پارامتر ارسال نگردد.

۳-۱-۳-۷ پاسخ درخواست غیرهمگام

پس از دریافت درخواست توسط سرور و بررسی مربوط به لایه انتقال پاسخ مناسب مطابق جداول (۸) و (۹) به کلاینت ارائه می شود.

جدول ۸. مدل داده پاسخ های غیرهمگام

اسم شی	AsynResponse
نوع فیلدها	<pre>{ "uid": "string", "referenceNumber": "string", "errorCode": "string", "errorDetail": "string" }</pre>

جدول ۹. توضیحات فیلدهای خروجی درخواست غیرهمگام

نام فیلد	توضیحات
uid	شناسه یکتای ارسال صورت حساب، شناسه ای که در سمت کلاینت هنگام ارسال صورت حساب تولید می شود.
referenceNumber	رسید یکتای دریافت صورت حساب، در صورتی که بسته با موفقیت توسط سرور دریافت شود، این شناسه به عنوان کد ارجاع برای کلاینت ارسال خواهد شد. به کمک این فیلد، وضعیت پردازش بسته قابل بررسی و پیگیری است. این کد سمت سرور تولید می شود.

نام فیلد	توضیحات
errorCode	کد خطا، در صورتی که دریافت بسته با خطایی مواجه شود، این فیلد پر شده و کد خطا بازگردانی می شود.
errorDetail	جزئیات خطا، در صورتی که دریافت بسته با خطایی مواجه شود، این فیلد پر شده و جزئیات خطا را شرح می دهد.



www.Hesabdary.Com
@HesabdaryCom

۲-۳-۷ متدهای همگام

۱-۲-۳-۷ سرویس درخواست های همگام

در جدول (۱۰) جزئیات ورودی و خروجی بسته های همگام بیان شده است.

لازم به ذکر است در متدهای همگام امضای درخواست ارسالی نیاز است و داده ها به رمزگذاری نیاز ندارند.

جدول ۱۰. درخواست های همگام

خروجی	ورودی داده	نام متد
token طول عمر توکن به ثانیه: expiresIn	شناسه یکنای حافظه یا : username شناسه شرکت معتمد	GET_TOKEN
نام تجاری: nameTrade وضعیت حافظه: fiscalStatus درصد حد مجاز: saleThreshold فروش شماره اقتصادی: economicCode	-	GET_FISCAL_INFORMATION
[[uid, referenceNumber, status, data, packetType, fiscalId }], ...]	{ UId: [{ uid, fiscalId } , { uid, fiscalId } , { uid, fiscalId }]	INQUIRY_BY_UID

خروجی	ورودی داده	نام متد
	<pre> }, ...]] </pre>	
<pre> [{ uid, referenceNumber, status, data, packetType, fiscalId }, ...] </pre>	<pre> { "referenceNumber": [referenceNumber_1, referenceNumber_2, referenceNumber_3, ...] } </pre>	INQUIRY_BY_REFERENCE_NUMBER
<pre> [{ uid, referenceNumber, status, data, packetType, fiscalId }, ...] </pre>	time	INQUIRY_BY_TIME
<pre> [{ uid, referenceNumber, status, data, packetType, fiscalId }, ...] </pre>	startDate: تاریخ شروع بازه مورد نظر endDate: تاریخ پایان بازه مورد نظر	INQUIRY_BY_TIME_RANGE
<pre> { "serverTime": "زمان سرور", "publicKeys": [{ "key": "کلید عمومی", "id": "شناسه کلید عمومی", "algorithm": "الگوریتم کلید", "purpose": "هدف کلید. ۱" }] "رمز گشایی صورت حسابها در جمع آوری" } </pre>	-	GET_SERVER_INFORMATION

خروجی	ورودی داده	نام متد
<pre>]] } </pre>		
<pre> { "result" : [{ "itemId": "شناسه کالا/خدمت", "tax": "نرخ مالیات بر ارزش افزوده" و سایر عوارض }, ...], "pagination": { "page": "صفحه جاری", "size": "تعداد در صفحه", "total": "تعداد کل", } } </pre>	<pre> { "filters": [لیست فیلتر بر روی داده ها], "orderBy": [لیست مرتب سازی], "page": "صفحه مورد درخواست", "size": "تعداد در صفحه", } </pre>	GET_SERVICE_STUFF_LIST
<p>nameTrade: نام تجاری</p> <p>taxpayerStatus: وضعیت مودی</p> <p>taxpayerType: نوع شخص</p> <p>postalcodeTaxpayer: کدهای پستی مودی</p> <p>addressTaxpayer: نشانی مودی</p>	economicCode	GET_ECONOMIC_CODE_INFORMATION

۲-۲-۳-۷ پاسخ درخواست های همگام

جدول ۱۱. توضیحات فیلدهای ساختار خروجی درخواست همگام

توضیحات	نام فیلد
شناسه یکتای ارسال صورتحساب، شناسه‌ای که در سمت کلاینت هنگام ارسال صورتحساب تولید می‌شود.	uid
نوع بسته پاسخ.	packetType
پاسخ رمز شده یا کشف بسته.	data

نام فیلد	توضیحات
encryptionKeyId	شناسه کلید عمومی حافظه مالیاتی، جهت باز کردن کلید متقارن. در صورتی که داده ها رمز نشده باشند، این فیلد خالی ارسال می شود.
symmetricKey	کلید متقارن رمز شده با کلید رمزنگاری (کلید عمومی سازمان) جهت باز کردن داده های رمز شده.
iv	بردار مقدار اولیه کلید.

۷-۳-۲-۳-متد دریافت توکن

کلاینت ها با استفاده از این متد، توکن JWT دریافت می کنند. با توجه به اینکه در این سرویس امضای درخواست کننده اجباری است، احراز هویت از طریق آن صورت می پذیرد. در صورتی که نام کاربری اعلام شده و امضای آن تطابق داشته باشد، توکن JWT برای کلاینت ارسال می شود. این توکن طول عمر مشخصی دارد، با منقضی شدن آن، کلاینت اقدام به دریافت توکن جدید می نمایند. با استفاده از این توکن در سرآیند درخواست ها می توان از این API ها استفاده کرد.

برای ارسال توکن ابتدا عبارت Bearer اضافه شده سپس توکن ارسال می شود. نمونه CURL درخواست در پیوست ۲-۲ ارائه شده است.

۷-۳-۲-۴-متد استعلام اطلاعات حافظه مالیاتی مودی و حد مجاز فروش مودی

با استفاده از این متد می توان اطلاعات حافظه مالیاتی مودی را دریافت نمود. این متد نیاز به احراز هویت دارد.

نمونه CURL درخواست در پیوست ۲-۳ ارائه شده است.

۷-۳-۲-۵-متد استعلام بسته های ارسالی غیر همگام

برای استعلام وضعیت صورتحساب های ارسال شده می توان از متدهای ذیل استفاده کرد: این متدها به احراز هویت نیاز دارند.

- Inquiry_by_uid: کلاینت می تواند با آرایه ای از UID ها، صورتحساب های مورد نظر خود را استعلام نماید. در پاسخ وضعیت آنها بازگردانده می شود.

نمونه CURL درخواست در پیوست ۲-۴-۱ ارائه شده است.

نکته: وجود fiscalId در ورودی درخواست کنار هر uid ضروری می باشد.

- Inquiry_by_reference_number: در این متد، کلاینت می تواند با آرایه ای از reference_number ها، صورتحساب های مورد نظر خود را استعلام نماید. در پاسخ وضعیت آنها باز گردانده می شود.

نمونه CURL درخواست در پیوست ۲-۴-۲ ارائه شده است.

- Inquiry_by_time: با این متد صورتحساب های دارای خطا از یک زمان مشخص تا زمان حال مشخص می شوند.

نمونه CURL درخواست در پیوست ۲-۴-۳ ارائه شده است.

- Inquiry_by_time_range: با این متد صورتحساب های دارای خطا در یک بازه زمانی مشخص می شوند.

نمونه CURL درخواست در پیوست ۲-۴-۴ ارائه شده است.

نکته: فیلد "time"، تاریخ شمسی با فرمت YYYYMMDD است و دقت شود فقط در خروجی این درخواست بسته هایی که وضعیت FAILED دارند برگشت داده می شوند.

۶-۲-۳-۷ متد دریافت اطلاعات سرور

این متد برای دریافت اطلاعات عمومی سرور شامل کلیدهای عمومی سازمان، شناسه کلید عمومی که از یک مرکز میانی معتبر اخذ شده است و تاریخ و زمان سرور، مورد استفاده قرار می گیرد. این متد به احراز هویت نیاز ندارد.

نمونه CURL درخواست در پیوست ۲-۵ ارائه شده است.

۷-۲-۳-۷ متد دریافت لیست کامل شناسه کالا/خدمات و نرخ مالیاتی

این متد برای دریافت لیست شناسه استاندارد کالاها و خدماتها که توسط وزارت صمت ابلاغ شده است مورد استفاده قرار می گیرد. با توجه به اینکه حجم نتیجه خروجی این متد ممکن است زیاد باشد، امکان دریافت

اطلاعات به صورت صفحه‌بندی شده نیز در نظر گرفته شده است. این متد نیاز به احراز هویت ندارد.

نمونه CURL درخواست در پیوست ۲-۶ ارائه شده است.

❖ ارسال فیلد فیلتر و مرتب سازی در ورودی اختیاری است. شماره صفحه از یک شروع میشود. برای

مثال اگر ۱۰ رکورد اول را بخواهیم دریافت کنیم ورودی به صورت زیر خواهد بود:

```
{
  "page": 1,
  "size": 10
}
```

۷-۳-۲-۸ متد استعلام اطلاعات شماره اقتصادی

این متد برای استعلام شماره اقتصادی مورد استفاده قرار می‌گیرد. این متد نیاز به احراز هویت ندارد.

نمونه CURL درخواست در پیوست ۲-۷ ارائه شده است.



۸- لیست خطاها

۸-۱ مدل داده خطاها

جدول ۱۲. ساختار خروجی پاسخ خطا

ErrorResponse	اسم شی
<pre>{ "errorDetail": "string", "errorCode": "string" }</pre>	نوع فیلدها

۸-۲ لیست خطاهای لایه انتقال

جدول ۱۳. خطاهای لایه انتقال

توضیحات	خطا	کد
خطای داخلی سرور	internal.server.error	۵۰۰۰
خطای general زمانی که بسته مشکل داشته و در سمت سرور خطایی به صورت مشخص وجود نداشته باشد	bad.request	۵۰۰۱
عدم دارا بودن دسترسی برای ارسال این درخواست	un.authorized	۵۰۰۲
ارسال uid با فرمت اشتباه در packet	uid.format.is.not.valid	۵۰۰۳
ساختار JSON درخواست اشتباه است	invalid.json.structure	۵۰۰۴
ارسال درخواست با uid تکراری در packet	duplicate.request.uid	۵۰۰۵
ارسال تعداد packet بیش از حد مجاز (در حال حاضر ۱۰۰ عدد)	packet.size.is.too.large	۵۰۰۶
عدم پشتیبانی از نوع packet ارسالی	not.supported.packet-type	۵۰۰۷
مقدار فیلد encryptionKeyId در ارسال رمز شده صورت حساب صحیح نمی باشد	encryption.key.id.not.valid	۵۰۰۸
عدم تطابق packet ارسالی با نوع درخواست sync	not.match.packet-type.with.request	۵۰۰۹
گذشت زمان مشخصی از زمان ارسال درخواست و دریافت آن توسط سرور	request.time.has.passed	۵۰۱۰
تکراری بودن requestTraceId در سرآیند درخواست	duplicate.request.trace.id	۵۰۱۱
پیدا نشدن اطلاعات حافظه مالیاتی ارسالی	fiscal.id.not.found	۵۰۱۲
عدم اعتبار امضای درخواست	invalid.packet.signature	۵۰۱۳
فرمت ساختار نادرست است	invalid.format	۵۰۱۴

توضیحات	خطا	کد
توکن نامعتبر	invalid.token	۵۰۱۵

۳-۸ لیست خطاهای لایه محتوا

جدول ۱۴. کدهای خطای دریافتی از هسته مالیاتی یا به عبارتی کدهای خطای لایه محتوا

ردیف	خطای واقع شده	شرح خطا
۱	عدم ثبت شماره اقتصادی فروشنده.	Seller economic code is empty
۲	عدم ثبت شماره اقتصادی خریدار در صورتحساب‌های الکترونیکی نوع اول.	Buyer economic code is empty
۳	عدم ثبت تاریخ و زمان صدور صورتحساب (میلادی).	Invoice date time is empty
۴	عدم ثبت تاریخ و زمان پرداخت صورتحساب در صورتحساب‌های الکترونیکی نوع سوم	Payment date time is empty
۵	عدم ثبت سریال صورتحساب.	Invoice number is empty
۶	عدم ثبت نوع صورتحساب.	Invoice type is empty
۷	عدم ثبت الگوی صورتحساب.	Invoice pattern is empty
۸	عدم ثبت موضوع صورتحساب.	Invoice subject is empty
۹	عدم ثبت شماره منحصر به فرد مالیاتی صورتحساب مرجع در صورتی که موضوع صورتحساب شامل اصلاحی، ابطالی و یا برگشت از فروش - یکی از مقادیر ۲، ۳ و ۴ باشد.	Reference tax-id is empty
۱۰	عدم ثبت شناسه کالا/خدمت.	Service-stuff-id is empty
۱۱	عدم ثبت مبلغ واحد.	Fee is empty
۱۲	عدم ثبت میزان ارز در صورتحساب‌های با الگوی فروش ارزی.	Currency-fee is empty
۱۳	عدم ثبت نرخ مالیات بر ارزش افزوده.	Vat rate is empty
۱۴	عدم ثبت تعداد/مقدار.	Amount is empty
۱۵	عدم ثبت شناسه یکتای ثبت قرارداد فروشنده در صورتحساب‌های الکترونیکی با الگوی قرارداد پیمانکاری.	Contract registration number is empty
۱۶	عدم ثبت شماره پروانه گمرکی فروشنده در صورتحساب‌های الکترونیکی با الگوی فروش ارزی.	Seller customs license is empty

ردیف	خطای واقع شده	شرح خطا
۱۷	عدم ثبت کد گمرک محل اظهار فروشنده در صورتحساب- های الکترونیکی با الگوی فروش ارزی.	Seller customs code is empty
۱۸	عدم ثبت نوع شخص خریدار.	Buyer type is empty
۱۹	عدم ثبت نوع پرواز در صورتحساب های الکترونیکی با الگوی بلیط هواپیما.	Flight type is empty
۲۰	عدم ثبت نوع ارز در صورتحساب های الکترونیکی با الگوی فروش ارزی.	Currency type is empty
۲۱	عدم ثبت نرخ برابری ارز با ریال در صورتحساب های الکترونیکی با الگوی فروش ارزی.	Exchange rate is empty
۲۲	عدم ثبت شماره اشتراک / شناسه قبض در صورتحساب های الکترونیکی با الگوی قبوض خدماتی.	Billing identification is empty
۲۳	عدم ثبت مبلغ قبل از تخفیف در صورتحساب های الکترونیکی با الگوی اول تا پنجم.	Pre-discount amount is empty
۲۴	عدم ثبت مبلغ تخفیف در صورتحساب های الکترونیکی با الگوی اول تا پنجم.	Discount amount is empty
۲۵	عدم ثبت مبلغ بعد از تخفیف در صورتحساب های الکترونیکی با الگوی اول تا پنجم (فروش-فروش ارزی- صورتحساب طلا، جواهر، پلاتین- قرارداد پیمانکاری-قبوض خدماتی).	After discount amount is empty
۲۶	عدم ثبت مبلغ مالیات بر ارزش افزوده.	Vat amount is empty
۲۷	عدم ثبت سهم مالیات بر ارزش افزوده از پرداخت در صورتحساب های الکترونیکی با الگوی اول تا چهارم (فروش-فروش ارزی- صورتحساب طلا، جواهر، پلاتین- قرارداد پیمانکاری).	Vat of payment is empty
۲۸	عدم ثبت روش تسویه در صورتحساب های الکترونیکی با الگوی اول تا چهارم (فروش-فروش ارزی- صورتحساب طلا، جواهر، پلاتین- قرارداد پیمانکاری).	Settlement method is empty
۲۹	عدم ثبت مبلغ کل کالا/خدمت.	Total service-stuff amount is empty

ردیف	خطای واقع شده	شرح خطا
۳۰	عدم ثبت مجموع مبلغ کل قبل از کسر تخفیف (به جز صورتحساب‌های الکترونیکی با الگوی بلیط هواپیما و صورتحساب‌های نوع سوم).	Total Pre-discount amount is empty
۳۱	عدم ثبت مجموع تخفیفات (به جز صورتحساب‌های الکترونیکی با الگوی بلیط هواپیما و صورتحساب‌های نوع سوم).	Total Discount amount is empty
۳۲	عدم ثبت مجموع مبلغ کل پس از کسر تخفیف (به جز صورتحساب‌های الکترونیکی با الگوی بلیط هواپیما و صورتحساب‌های نوع سوم).	Total After discount amount is empty
۳۳	عدم ثبت مجموع مالیات بر ارزش افزوده.	Total Vat amount is empty
۳۴	عدم ثبت مجموع سایر مالیات، عوارض و وجوه قانونی.	Total other-duty amount is empty
۳۵	عدم ثبت مجموع صورتحساب.	Total bill is empty
۳۶	عدم ثبت مجموع سهم مالیات بر ارزش افزوده از پرداخت.	Total Vat of payment is empty
۳۷	عدم رعایت قالب فایل متنی ارسالی.	JSON file is invalid
۳۸	شماره منحصر به فرد مالیاتی نامعتبر	Invalid tax-id
۳۹	سریال صورتحساب ارسالی نامعتبر	Invalid invoice number
۴۰	شماره منحصر به فرد مالیاتی صورتحساب مرجع نامعتبر	Invalid reference tax-id
۴۱	عدم رعایت مهلت زمانی ابلاغی صدور صورتحساب اصلاحی، ابطالی و برگشت از فروش	Invalid invoice date time
۴۲	تاریخ و زمان صدور صورتحساب نامعتبر (وارد کردن زمان آینده)	Invalid invoice date time
۴۳	نوع صورتحساب نامعتبر	Invalid invoice type
۴۴	الگوی صورتحساب نامعتبر	Invalid invoice pattern
۴۵	شماره اقتصادی فروشنده نامعتبر	Invalid seller economic code
۴۶	شماره اقتصادی خریدار نامعتبر	Invalid buyer economic code
۴۷	عدم تکمیل فیلدهای ضروری مرتبط با الگو	Essential field is empty
۴۸	شناسه یکتای ثبت قرارداد فروشنده نامعتبر	Invalid Contract registration number
۴۹	شناسه کالا/خدمت نامعتبر	Invalid Service-stuff-id
۵۰	واحد اندازه‌گیری نامعتبر (کدهای آن در جدول واحد وجود نداشته باشد)	Invalid measurement unit

ردیف	خطای واقع شده	شرح خطا
۵۱	نوع ارز نامعتبر (فقط در الگوی فروش ارزی صورتحساب نوع اول و دوم)	Invalid currency type
۵۲	خطا در محاسبه محدوده مجاز ارقام	Error in digit ranges
۵۳	روش تسویه نامعتبر (فقط در صورتحساب الگوهای ۱،۲،۳، ۴ و ۶ نوع اول)	Invalid Settlement method
۵۵	موضوع صورتحساب نامعتبر	Invalid invoice subject
۵۶	خطای نوع مقدار وارد شده مغایر با نوع فیلد	Invalid Data type
۵۷	تکراری بودن فیلد «شماره منحصر به فرد مالیاتی صورتحساب»	Duplicate tax id
۵۸	عدم تطابق فیلد «نوع شخص خریدار» با اطلاعات خریدار در سامانه	Mismatch buyer info
۵۹	فیلد «شماره اقتصادی فروشنده» با شناسه حافظه مالیاتی، مغایرت دارد.	Mismatch seller economic code and fiscal Id
۶۰	مقدار فیلد شناسه حافظه مالیاتی (fiscal Id) در صورتحساب با شناسه حافظه مالیاتی موجود در فیلد شماره منحصر به فرد مالیاتی (taxId) تطابق ندارند	Tax id and fiscal Id does not match
۶۱	شماره اقتصادی فروشنده، موجود در اقلام صورتحساب (tins) و شناسه حافظه مالیاتی موجود در فیلد شماره منحصر به فرد مالیاتی taxId تطابق ندارند	Seller Economic code and fiscal Id does not match

پیوست ۱

۱-۱ کد نورمالسازی JSON به زبان java

```
import com.fasterxml.jackson.core.JsonProcessingException;
import com.fasterxml.jackson.databind.ObjectMapper;

import java.text.Collator;
import java.util.*;

public class CryptoUtils {

    private final static ObjectMapper mapper = new ObjectMapper();

    public static byte[] hexStringToByteArray(String s) {
        int len = s.length();
        byte[] data = new byte[len / 2];
        for (int i = 0; i < len; i += 2) {
            data[i / 2] = (byte) ((Character.digit(s.charAt(i), 16) << 4)
                + Character.digit(s.charAt(i + 1), 16));
        }
        return data;
    }

    public static String normalJson(Object object, Map<String, Object> header) {

        if (object == null && header == null)
            return null;
    }
}
```

```
Map<String, Object> map = null;

if (object != null) {
    if (object instanceof String) {
        try {
            object = mapper.readValue((String) object, Object.class);
        } catch (JsonProcessingException e) {
            throw new RuntimeException(e.getMessage());
        }
    }
}

if (object instanceof Collection) {
    PacketsWrapper packetsWrapper = new PacketsWrapper((Collection) object);
    map = mapper.convertValue(packetsWrapper, Map.class);
} else {
    map = mapper.convertValue(object, Map.class);
}

if (map == null && header != null) {
    map = header;
}

if (map != null && header != null) {
    for (Map.Entry<String, Object> entry : header.entrySet()) {
        map.put(entry.getKey(), entry.getValue());
    }
}

Map<String, Object> result = new HashMap<>();
```

```
flatMap(result, null, map);

StringBuilder sb = new StringBuilder();
List<String> keys = new ArrayList<>(result.keySet());
Collections.sort(keys, Collator.getInstance(Locale.ENGLISH));
for (String key : keys) {
    String textValue;
    Object value = result.get(key);
    if (value != null) {
        textValue = value.toString();
        if (textValue == null || textValue.equals("")) {
            textValue = "#";
        } else {
            textValue = textValue.replaceAll("#", "##");
        }
    } else {
        textValue = "#";
    }
    sb.append(textValue).append('#');
}
return sb.deleteCharAt(sb.length() - 1).toString();
}

private static String getKey(String rootKey, String myKey) {
    if (rootKey != null) {
        return rootKey + "." + myKey;
    } else {
        return myKey;
    }
}
```



```
}  
  
private static void flatMap(Map<String, Object> result, String rootKey,  
Object input) {  
    if (input instanceof Collection) {  
        Collection list = (Collection) input;  
        int i = 0;  
        for (Object e : list) {  
            String key = getKey(rootKey, "E" + i++);  
            flatMap(result, key, e);  
        }  
    } else if (input instanceof Map) {  
        Map<String, Object> map = (Map) input;  
        for (Map.Entry<String, Object> entry : map.entrySet()) {  
            flatMap(result, getKey(rootKey, entry.getKey()), entry.getValue());  
        }  
    } else {  
        result.put(rootKey, input);  
    }  
}  
  
private static class PacketsWrapper {  
    private Collection packets;  
    public PacketsWrapper() {  
    }  
    public PacketsWrapper(Collection packets) {  
        this.packets = packets;  
    }  
    public Collection getPackets() {  
        return packets;  
    }  
}
```

```
public void setPackets(Collection packets) {
    this.packets = packets;
}
}
```

◀ در کلاس CryptoUtils در کد بالا می توانید از متد استاتیک normalJson استفاده کنید.

۲-۱ کد DotNet برای نورمالسازی JSON

```
using Newtonsoft.Json;
using Newtonsoft.Json.Linq;
using System;
using System.Collections;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using Org.BouncyCastle.Crypto;
using Org.BouncyCastle.Crypto.Engines;
using Org.BouncyCastle.Crypto.Modes;
using Org.BouncyCastle.Crypto.Parameters;
using Org.BouncyCastle.OpenSsl;
using Org.BouncyCastle.Security;
using System.Security.Cryptography;
using System.IO;
using tax_collect_data_sdk_dotnet;

namespace ir.tax.gov.sdk.util
{
    public class CryptoUtils
```

```
{  
    public static byte[] StringToByteArray(string hex)  
    {  
        return Enumerable.Range(0, hex.Length)  
            .Where(x => x % 2 == 0)  
            .Select(x => Convert.ToByte(hex.Substring(x, 2), 16))  
            .ToArray();  
    }  
  
    public static string NormalJson(object obj, Dictionary<string, string>  
header)  
    {  
        if (obj == null && header == null)  
            throw new AccessViolationException();  
        Dictionary<string, object> map = null;  
        if (obj != null)  
        {  
            if (obj.GetType() == typeof(string))  
            {  
                if (obj.ToString().Trim().StartsWith("[")  
                {  
                    obj = ToList<object>((string)obj);  
                }  
                else  
                {  
                    obj = JsonConvert.DeserializeObject<object>((string)obj);  
                }  
            }  
            if (obj.GetType().IsGenericType &&  
obj.GetType().GetGenericTypeDefinition() == typeof(List<>))  
            {
```

```
    PacketsWrapper packetsWrapper = new PacketsWrapper(obj);
    map = ToDictionary<object>(packetsWrapper);
}
else
{
    map = ToDictionary<object>(obj);
}
}
if (map == null && header != null)
{
    map = new Dictionary<string, object>();
    foreach (var headerElem in header)
        map.Add(headerElem.Key, headerElem.Value.ToString());
}
if (map != null && header != null)
{
    foreach (var headerElem in header)
        map.Add(headerElem.Key, headerElem.Value);
}
Dictionary<string, object> result = new Dictionary<string, object>();
result =
JsonHelper.DeserializeAndFlatten(JsonConvert.SerializeObject(map));
StringBuilder sb = new StringBuilder();
HashSet<string> keysSet = new HashSet<string>(result.Keys);
if (keysSet == null || !keysSet.Any())
{
    return null;
}
var keys = keysSet.OrderBy(x => x).ToList();
```

```
foreach (var key in keys)
{
    string textValue;
    object value;
    if (result.TryGetValue(key, out value))
    {
        if (value != null)
        {
            if (value.Equals(true) || value.Equals(false) ||
value.ToString().Equals("False") || value.ToString().Equals("True"))
            {
                textValue = value.ToString().ToLower();
            }
            else
            {
                textValue = value.ToString();
            }
            if (textValue == null || textValue.Equals(""))
            {
                textValue = "#";
            }
            else
            {
                textValue = textValue.Replace("#", "##");
            }
        }
        else
        {
            textValue = "#";
        }
    }
}
```

```
    }  
    }  
    else  
    {  
        textValue = "#";  
    }  
    sb.Append(textValue).Append('#');  
    }  
    return sb.Remove(sb.Length - 1, 1).ToString();  
    }  
    private static string getKey(string rootKey, string myKey)  
    {  
        if (rootKey != null)  
        {  
            return rootKey + "." + myKey;  
        }  
        else  
        {  
            return myKey;  
        }  
    }  
    }  
  
    public static Dictionary<string, TValue> ToDictionary<TValue>(object obj)  
    {  
        var json = JsonConvert.SerializeObject(obj);  
        var dictionary = JsonConvert.DeserializeObject<Dictionary<string,  
TValue>>(json);  
        return dictionary;  
    }  
    }
```

```

public static List<Dictionary<string, object>> ToList<TValue>(string obj)
{
    var dictionary = JsonConvert.DeserializeObject<List<Dictionary<string,
object>>>(obj);
    return dictionary;
}
}
}

```

کد بالا از کلاس دیگری به نام JSONHelper استفاده می کند که در ادامه آورده شده:

```

using Newtonsoft.Json;
using Newtonsoft.Json.Linq;
using System;
using System.Collections.Generic;
using System.IO;
using System.Linq;
using System.Text;

namespace ir.tax.gov.sdk.util
{
    public class JsonHelper
    {
        public static Dictionary<string, object> DeserializeAndFlatten(string json)
        {
            Dictionary<string, object> dict = new Dictionary<string, object>();

            JToken token = JToken.ReadFrom(new JsonTextReader(new
StringReader(json)));

            FillDictionaryFromJToken(dict, token, "");

            return dict;
        }
    }
}

```

```
private static void FillDictionaryFromJToken(Dictionary<string, object>
dict, JToken token, string prefix)
{
    switch (token.Type)
    {
        case JTokenType.Object:
            foreach (JProperty prop in token.Children<JProperty>())
            {
                FillDictionaryFromJToken(dict, prop.Value, Join(prefix, prop.Name));
            }
            break;
        case JTokenType.Array:
            int index = 0;
            foreach (JToken value in token.Children())
            {
                FillDictionaryFromJToken(dict, value, Join(prefix, index.ToString()));
                index++;
            }
            break;
        default:
            dict.Add(prefix, ((JValue)token).Value);
            break;
    }
}

private static string Join(string prefix, string name)
{
    return (string.IsNullOrEmpty(prefix) ? name : prefix + "." + name);
}
}
```


}

در کلاس CryptoUtils می توانید از متد NormalJson برای نرمالسازی JSON مدنظر استفاده کنید.

۳-۱ روش امضا رشته (string)

۱-۳-۱ کد جاوا

```
public static String getSignedText(String text, String algorithm, PrivateKey
privateKey) throws UnsupportedOperationException, NoSuchAlgorithmException,
InvalidKeyException, SignatureException {
    byte[] data = text.getBytes("UTF8");

    Signature sig = Signature.getInstance(algorithm == null ? "SHA256WITHRSA"
: algorithm);
    sig.initSign(privateKey);
    sig.update(data);
    byte[] signatureBytes = sig.sign();
    return Base64.getEncoder().encodeToString(signatureBytes);
}
```



۲-۳-۱ کد C#

```
public static string SignData(String stringToBeSigned, string
privateKey)
{
    var pem = "-----BEGIN PRIVATE KEY-----\n" + privateKey + "\n-----
END PRIVATE KEY-----"; // Add header and footer
```

```
PemReader pr = new PemReader(new StringReader(pem));
AsymmetricKeyParameter privateKeyParams =
(AsymmetricKeyParameter)pr.ReadObject();
RSAParameters rsaParams =
DotNetUtilities.ToRSAParameters((RsaPrivateCrtKeyParameters)privateKeyParams)
;

RSACryptoServiceProvider csp = new RSACryptoServiceProvider();//
cspParams);
csp.ImportParameters((RSAParameters)rsaParams);

var dataBytes = Encoding.UTF8.GetBytes(stringToBeSigned);
return Convert.ToBase64String(csp.SignData(dataBytes,
HashAlgorithmName.SHA256, RSASignaturePadding.Pkcs1));
}
```

۱-۴ کد روش رمزگذاری به روش متقارن AES/ GCM

۱-۴-۱ کد جاوا:

◀ متد نحوه ایجاد کلید متقارن Random:

```
public static SecretKey getAESKey(int keysize) throws
NoSuchAlgorithmException {
    KeyGenerator keyGen = KeyGenerator.getInstance("AES");
    keyGen.init(keysize, SecureRandom.getInstanceStrong());
    return keyGen.generateKey();
}
```

◀ متد ایجاد یک مقدار Random مورد استفاده در رمزنگاری متقارن (IV)

```
public static byte[] getRandomNonce(int byteSize) {
    byte[] nonce = new byte[byteSize];
    new SecureRandom().nextBytes(nonce);
    return nonce;
}
```

◀ نحوه رمزنگاری با استفاده از SecretKey و IV

```
public static byte[] encrypt(byte[] pText, SecretKey secret, byte[] iv)
throws Exception {
    Cipher cipher = Cipher.getInstance("AES/GCM/NoPadding");
    cipher.init(Cipher.ENCRYPT_MODE, secret, new GCMParameterSpec(128, iv));
    return cipher.doFinal(pText);
}
```

◀ کد نحوه XOR کردن دو آرایه

```
public static byte[] xor(byte[] a, byte[] b) {
    int aLen = a.length;
    int bLen = b.length;
    int min = 0;
```

```

int size = aLen > bLen ? aLen : bLen;
byte[] c = new byte[size];

if (size == aLen) {
    min = bLen;
    System.arraycopy(a, min, c, min, size - min);
} else {
    min = aLen;
    System.arraycopy(b, min, c, min, size - min);
}

for (int i = 0; i < min; i++) {
    c[i] = (byte) (a[i] ^ b[i]);
}

return c;
}

```

C# ۲-۴-۱ کد

در C# می‌توانید با `byte[]` به صورت کاملاً تصادفی دو کلید `IV` و `Secret Key` را ایجاد کنید و از

روش زیر متن خود را `encrypt` کنید:

```

public static string AesEncrypt(byte[] payload, byte[] key, byte[] iv)
{
    var cipher = new GcmBlockCipher(new AesEngine());

    byte[] baPayload = new byte[0];

    cipher.Init(true, new AeadParameters(new KeyParameter(key), 128, iv,
    baPayload));

    var cipherBytes = new byte[cipher.GetOutputSize(payload.Length)];

    int len = cipher.ProcessBytes(payload, 0, payload.Length, cipherBytes, 0);
}

```

```

cipher.DoFinal(cipherBytes, len);
return Convert.ToBase64String(cipherBytes);
}

public static byte[] Xor(byte[] left, byte[] right)
{ /*from w w w . j a v a 2 s . c o m*/
    byte[] val = new byte[left.Length];
    for (int i = 0; i < left.Length; i++)
        val[i] = (byte)(left[i] ^ right[i]);
    return val;
}

```

۵- کد روش رمزگذاری به روش نامتقارن RSA-OAEP-SHA256

۱-۵-۱ کد جاوا

```

public static String encrypt(String text, PublicKey publicKey) throws
NoSuchPaddingException, NoSuchAlgorithmException, BadPaddingException,
IllegalBlockSizeException, InvalidKeyException {
    Cipher encryptCipher = Cipher.getInstance("RSA/ECB/OAEPWITHSHA-
256ANDMGF1PADDING");
    encryptCipher.init(Cipher.ENCRYPT_MODE, publicKey);

    byte[] secretMessageBytes = text.getBytes(StandardCharsets.UTF_8);
    byte[] encryptedMessageBytes = encryptCipher.doFinal(secretMessageBytes);
    return Base64.getEncoder().encodeToString(encryptedMessageBytes);
}

```

۱-۵-۲ کد C#

```

public static string EncryptData(String stringToBeEncrypted, string
publicKey)
{
    try
    {

```

```

        //var pem = "-----BEGIN PUBLIC KEY-----\n" + publicKey + "\n-
        ----END PUBLIC KEY-----";        // Add header and footer
        AsymmetricKeyParameter asymmetricKeyParameter =
        PublicKeyFactory.CreateKey(Convert.FromBase64String(publicKey));
        RsaKeyParameters rsaKeyParameters =
        (RsaKeyParameters)asymmetricKeyParameter;
        RSAParameters rsaParameters = new RSAParameters();
        rsaParameters.Modulus =
        rsaKeyParameters.Modulus.ToByteArrayUnsigned();
        rsaParameters.Exponent =
        rsaKeyParameters.Exponent.ToByteArrayUnsigned();
        RSACng rsa = new RSACng();
        rsa.ImportParameters(rsaParameters);

        string base64 =
        Convert.ToBase64String(rsa.Encrypt(Encoding.UTF8.GetBytes(stringToBeEncrypted
        ), RSAEncryptionPadding.OaepSHA256));

        if (base64.Length % 4 == 3 )
        {
            base64 += "=";
        } else if (base64.Length % 4 == 2)
        {
            base64 += "==";
        }
        return base64;
    }
    catch (Exception e)
    {
        return "error";
    }
}

```



```

oa6QQGZPyad1AKQJMZtR1UKR/1VKgHaKfyqqQGGdmgOjm1HUy+5Lm4J911Z8ETqs0sS383T06BNiF
HT1X+ApFn8UbM3gKORiA1e5F8v4I5e7dqTb+et2Ivxee5TEkNXZXJoMGXFrQE/bho0W8A9kGi/ye1
udMcoxczmYSxWXXSdSbn1THstcT7Fa2G31c1w0LDdVsq20yCK9vGCMqSnu9PMrefUb/3jP/a71d15
ecSN1QDbGdZ03ASKVQ8b356cuW6yuqECbvq1EeI1J1bB9T3wthKRvTcVR1TYvrLzf8ebdjAmysc+h
rgnQ1FuJnwxoX6wXfnw+2ph1KMiaPrLH6p+bnm7+AUiaGu/LuSdBJPzYNQ0EIrkJ5S5DrJi5KHn9jD
4b3gCQ97B8qspBspvd3mYLLVHQGU+qa4GP5EdoiU76vFzAHSHu+TOTDmKs9NQ7jUwuFlUov3+Fx/M
LhUYkwyDogbwGiyauK5wdgwhUi4AmBR8SwnMG/TxGIdB7xIsMydNOJOctKDJzTK0odvd4d7VkosN
wVzhQw6C9okLJmBblnJbJQt0QZN5MIzXG6MfGkgbJ6g/zFPRKJf7+X9u9Vt83uUCx3ftrmdff/9uN
+5hbVep2gyxmMmiq4Lw2uKg8vyRSzDe7iAckfQWX02Vstb1U3ZIT2iCzVNGyEYgsLLQdV08yIjn8P
fIuGsytMAQx9iH2Q32rZqhB8vGsJQwBznKywv/u5wYRj1LVEN1dgGoqfXgjFdbdhjBzXLgbbLQ8+
FVi0GfCY88mRRKtkmzLnGJtwTenaNCsfrDDg7Be0/SCzuqij2P0r6W0V2X7zCQWKCThTWUWRu0IM0
nCdRIoshg2U2E/IQ+AIt4oQWjIF0QSy2cY4GUuVPXgwiFNvKV3xkYE3Yyfeg1PhJskj1Wnth9+V17
/C2IBGxXXVQxoLLgheq6IMLARz6N0bvkX4y0Z2PE0C0fpwYxBxEop6SdV4hFy3mZ1C5Wg4FaccfoG
EJRpfCuYT59cIMF1xquwuMRyRBXrfgGzOdZe/1I41/snweEqbXG2bXM/24/W0hdD3rR0X0+K+wms0
bkoBUyTamhZDI8uuaHTYx1zQ/SJ9BgaV6C70s+K7jiUjXJgc0yinsmsk0B3yoq5tCqpIfcyZ5hbHw
R7Vqc+2TgtygmQXMjg+Tu301j3J/Xqse6UoFy+RTM0hEmfMyGmMxQeX4X2IZ5fa98hg1Pdsdrvm4J
mDvfjDnLCOpLDNeHqvEhKj8p9Kmxwdox61V058UeWwZA5ZH70/Krk+Ndfzua1g=",
  "encryptionKeyId": "31cf3e11-c468-4b14-90a4-d7c8c7e72fd5",
  "symmetricKey":
"cbAkPRW8JJiouZM0zLgiqIgtajUcW1Nr2CoZj6uH4ESMIfJjTgR7kd0j5msAlb1f5vcN21AYtv3
3+UHNipM0bAq30QIF9TnCOgNY+fba1FHQ15Em7/VE+5WYEr+N5uPnRHX/JK2j/A2/jiwwYmi9+Gey
FK2QQYGLUYrFPuW+ifUG1veJldPAocwkD1RxZVXp+hV1L2fKxSwDUCVF5Uvr5jX8ACwmMa8t5qCco
w/xWxumod1BfE9sPOUonOZ1hVINscJYrN4y7MG0Re88F/WRyL4grznetSSK0sAGTrGVf1KZ1Mm3ng
DF+o+8+t1WtVzF5Hj0zv60DAix3ikS03efMbFtGGQ5WygoEhhWlgt9/CqjkEm7qHE5T0iQ+pE+f1o
TNXfh4eGH/+j9zeI//uLxcHSH/TnTmUlGxlareNXakumtcrKKu1NAw2Mm7F+XBLKXXMfw3iJrTPd3
/hpycPTVpu/6SO/7JMKUA44+irWw5AaX17j4EDWF72AvVDJCP1h2Qw7Krw7u4HFET3Q115L2vuP/E
TWvFVgBitP5DbdB9nFoSb8NwKZn6AqGgYaLOVz+8Y8SHgEBueix3V4e5PIm31WTbViqgnANP4TVft
T3ZL3b3yBkjvQpvc2CtstXgG05C16FzWX16UiR+IYZ7ahOolaTwmZr+GJA87ZLjKaK4=",
  "iv": "dee90162e26db3f2246f052f38168ed0", "dataSignature":
"VSvyWrpmT1TwI8I1vUue9wF0EGNFMZ/2dPgM1tj00vr8agPDHoT0iL5J3XxqvfCauCOfaFs6iVpw
dccwAtXfsFJ4wNQF3Mqr1I9un1v5AEePPEXAU46CK14Ny5sm3WGDtdnezx1+4FBCv05uP07RkeDw
ASyYOySfdw19d6fHes7KNkaLW72NetbTaZwytQtHx7ib+7cJyG+54eLAY3L6EIuoNiRSI1C1Pn53Q
8AT90uRV8UPSCcpiZhg/YINQXrunF2YH/LbTSqckwFsdukqg6BGZJbaqPwMfvm2WdPZLNTEW/BgNm
2SmSNwxqivQb1AY2mcfNg06dkyDCRVWTUeA==",
  "fiscalId": "AA56CD"
}],
"signature":
"FohMakKq0WRMPQD0nStssK2iP0bbFojw7w+NVUoWjTdyRFNeKBQeLP9FpL3r5u6EliSKUi03vu1I
vBzEbAaFBuEHSbmyr3q0TN0CpuORdzqHDT/onk/evvpOoEFt3LvowfLBoxNLDhAGrzD1K56j1Rco9
3U4ip1JgKzFmm9h1mByzTfDEe9FLX/22Gy9regeYtTg9sc12URu7csVttUr8YjCqFxuR8214m0tZd
Rf6jR709YZmskarPXavPsDr8buz7dz0HI0hIeok0vToyG3J1bAVM10SdWREq1Ix0czJ5jLnMiI8N3
1s8rvnypKzo5yWDOjXECTrLFRr+8MgK42Sw=="
}'

```

• نمونه پاسخ درخواست بالا :


```
{
  "signature": "",
  "signatureKeyId": "",
  "timestamp": 1652605524,
  "result": [
    {
      "uid": "8a00f17a-bd35-46bc-ae52-3f61fab868c2",
      "referenceNumber": "967072eb-203e-428e-b9bb-6d2efdb9d356",
      "errorCode": null,
      "errorDetail": null
    }
  ]
}
```

• نمونه پاسخ درخواست در صورت رخداد خطا:

```
{
  "signature": "",
  "signatureKeyId": "",
  "timestamp": 1652605524,
  "result": [
    {
      "uid": "8a00f17a-bd35-46bc-ae52-3f61fab868c2",
      "referenceNumber": null,
      "errorCode": "5008",
      "errorDetail": "invalid.request.uid"
    }
  ]
}
```

۲-۲-۲ متد دریافت توکن

• نمونه CURL:

```
curl --location --request POST
'https://tp.tax.gov.ir/req/api/tsp/sync/GET_TOKEN' \
--header 'requestTraceId: 1655185848687' \
--header 'timestamp: 1655185848687' \
--header 'Content-Type: application/json' \
--data-raw '{
  "time": 1,
  "packet": {
    "uid": null,
```

```

    "packetType": "GET_TOKEN",
    "retry": false,
    "data": {
      "username": "test-tsp-id-1"
    },
    "encryptionKeyId": "",
    "symmetricKey": "",
    "iv": "",
    "fiscalId": "",
    "dataSignature": ""
  },
  "signature":
  "IiIdkclswu3Krc8ZM7MqvEy7ZWzJmBPSl1CQrI0dhLGdRPRmomVo+UkbdzRyuth9G4Enbg0jnjz
  5WJcF08MuBVouASTMfv/OC0hAkxTudQtWzU00d6BU/YiRT5a1Nwdey0dMsn3T083luLv9iG/1KKz9
  ewUem0RwBY0nehD6rJFXHirGDfJPHB0TSHCqHL1vQe0JLZAQwaTTieEE8zNWxNr53BS2KxRKX8+M
  leoU18LWUn6wZS/zs3auOKSRS05pgJVq6zZCadd5D7v1hrw1KB/Xf04pv8GexAx2dbRMiGG5eumQG
  BcLo1RvJW2mZsGu+dQRm/NwnIpN7CP5qlkg=="
}'

```

- نمونه پاسخ درخواست:

```

{
  "signature": null,
  "signatureKeyId": null,
  "timestamp": 1655185988494,
  "result": {
    "uid": null,
    "packetType": "TOKEN_RESULT",
    "data": {
      "token":
      "eyJhbGciOiJIUzUxMiJ9.eyJjbGlbnRUeXB1IjoiveFNQIiwidG9rZW5JZCI6IjZlODlhZDQ3L
      TB1ZjQtNDRmNC05YWZkLWI5MjdlNDMlZmI2NyIsInBlcm1pc3Npb25zIjpbInRzcC5hc3luYy5m
      YXN0LWVucXVldWUilCj0c3AuYXN5bmMubm9ybWFsLWVucXVldWUilCj0c3Auc3luYyJdLCJwYW
      NrZXRUeXB1cyI6WyJHRVRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIklOUVVJU1lfQ1lfVE
      lNRSIsIkdFVF9TRVJWVjJfSU5GT1JNQRVJT04iLCJ0c3luYyJdLCJwYWNRZXRUeXB1cyI6WyJHR
      VRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkdFVF9TRVJWVjJfSU5GT1JNQRVJT04iLC
      J0c3luYyJdLCJwYWNRZXRUeXB1cyI6WyJHRVRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkd
      FVF9TRVJWVjJfSU5GT1JNQRVJT04iLCJ0c3luYyJdLCJwYWNRZXRUeXB1cyI6WyJHRVRfRUNPTk
      9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkdFVF9TRVJWVjJfSU5GT1JNQRVJT04iLCJ0c3luYyJdLC
      JwYWNRZXRUeXB1cyI6WyJHRVRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkdFVF9TRVJW
      SUNF1NUVUZGX0xJU1QiXSwiaXNzIjoiveFEVFIe9yZ2FuaXphdGlviIsImlkIjoidGVzdC10c3Ata
      WQtMSIsImV4cCI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0
      ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTI
      0MDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY
      3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF
      0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1
      NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0
      wii",
      "signature": null,
      "signatureKeyId": null,
      "timestamp": 1655185988494,
      "result": {
        "uid": null,
        "packetType": "TOKEN_RESULT",
        "data": {
          "token":
          "eyJhbGciOiJIUzUxMiJ9.eyJjbGlbnRUeXB1IjoiveFNQIiwidG9rZW5JZCI6IjZlODlhZDQ3L
          TB1ZjQtNDRmNC05YWZkLWI5MjdlNDMlZmI2NyIsInBlcm1pc3Npb25zIjpbInRzcC5hc3luYy5m
          YXN0LWVucXVldWUilCj0c3AuYXN5bmMubm9ybWFsLWVucXVldWUilCj0c3Auc3luYyJdLCJwYW
          NrZXRUeXB1cyI6WyJHRVRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIklOUVVJU1lfQ1lfVE
          lNRSIsIkdFVF9TRVJWVjJfSU5GT1JNQRVJT04iLCJ0c3luYyJdLCJwYWNRZXRUeXB1cyI6WyJHR
          VRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkdFVF9TRVJWVjJfSU5GT1JNQRVJT04iLC
          J0c3luYyJdLCJwYWNRZXRUeXB1cyI6WyJHRVRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkd
          FVF9TRVJWVjJfSU5GT1JNQRVJT04iLCJ0c3luYyJdLCJwYWNRZXRUeXB1cyI6WyJHRVRfRUNPTk
          9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkdFVF9TRVJWVjJfSU5GT1JNQRVJT04iLCJ0c3luYyJdLC
          JwYWNRZXRUeXB1cyI6WyJHRVRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkdFVF9TRVJW
          SUNF1NUVUZGX0xJU1QiXSwiaXNzIjoiveFEVFIe9yZ2FuaXphdGlviIsImlkIjoidGVzdC10c3Ata
          WQtMSIsImV4cCI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF
          0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1
          NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0
          wii",
          "signature": null,
          "signatureKeyId": null,
          "timestamp": 1655185988494,
          "result": {
            "uid": null,
            "packetType": "TOKEN_RESULT",
            "data": {
              "token":
              "eyJhbGciOiJIUzUxMiJ9.eyJjbGlbnRUeXB1IjoiveFNQIiwidG9rZW5JZCI6IjZlODlhZDQ3L
              TB1ZjQtNDRmNC05YWZkLWI5MjdlNDMlZmI2NyIsInBlcm1pc3Npb25zIjpbInRzcC5hc3luYy5m
              YXN0LWVucXVldWUilCj0c3AuYXN5bmMubm9ybWFsLWVucXVldWUilCj0c3Auc3luYyJdLCJwYW
              NrZXRUeXB1cyI6WyJHRVRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIklOUVVJU1lfQ1lfVE
              lNRSIsIkdFVF9TRVJWVjJfSU5GT1JNQRVJT04iLCJ0c3luYyJdLCJwYWNRZXRUeXB1cyI6WyJHR
              VRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkdFVF9TRVJWVjJfSU5GT1JNQRVJT04iLC
              J0c3luYyJdLCJwYWNRZXRUeXB1cyI6WyJHRVRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkd
              FVF9TRVJWVjJfSU5GT1JNQRVJT04iLCJ0c3luYyJdLCJwYWNRZXRUeXB1cyI6WyJHRVRfRUNPTk
              9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkdFVF9TRVJWVjJfSU5GT1JNQRVJT04iLCJ0c3luYyJdLC
              JwYWNRZXRUeXB1cyI6WyJHRVRfRUNPTk9NSUNfQ09ERV9JTkZPuk1BVElPTiIsIkdFVF9TRVJW
              SUNF1NUVUZGX0xJU1QiXSwiaXNzIjoiveFEVFIe9yZ2FuaXphdGlviIsImlkIjoidGVzdC10c3Ata
              WQtMSIsImV4cCI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF
              0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1
              NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0wiY3JlYXRlRGF0ZSI6MTY1NTIwMDM4O0
              wii"
            }
          }
        }
      }
    }
  }
}

```



```
X0xJU1QiXSwiaXNzIjoiVEFYIE9yZ2FuaXphdGlvbiIsImlkIjoidGVzdC10c3AtawQtMSI5ImV
4cCI6MTY1NTIwMDM4OCwiY3JlYXRlRGF0ZSI6MTY1NTE4NTk4ODQ5Mn0.SF06IpHsdSEKHDC0Vl
X7oqgVITzy5S3ksehSHSbdrfwiaYxDt1mMn541TV8zP-HowhBs8u1fjs_S81kiZON4FA' \
--header 'Content-Type: application/json' \
--data-raw '{
  "time": 1,
  "packet": {
    "uid": null,
    "packetType": "INQUIRY_BY_UID",
    "retry": false,
    "data": [
      {"uid": "3b33584c-331e-4fbc-97ea-8d294a2009db", "fiscalId":
"AA56CD"}
, {"uid": "8d595073-6349-423e-847f-83ae8a126394", "fiscalId": "AA56CD"}
, {"uid": "c0b286fd-b30f-49d7-97ca-640e91652f6f", "fiscalId": "AA56CD"}
],
    "encryptionKeyId": "",
    "symmetricKey": "",
    "iv": "",
    "fiscalId": "",
    "dataSignature": ""
  },
  "signature":
"Vny+goEh3eDH1HCijyvD7LLvUi+iAJEmgk18jc1yp73SrNHZ0RHaFbsgXICN5F52zV8HPfa3YI
cddBi3ZjVNVs9RA+HsEHolavOecPLo9A0IGS7y+BtVv1FBKLtizbflpejprSvN781edJQmEsjg
MMiVZA1zexQ8HU73/kf3fIyaviXXVyVcwM7DFqiyVdVV4IX3kljYVzyamU08PD19zTcwQMxwiSd
QiQ/plZtx0wzP2UTyLmy47jskdJVjpDseM1iSEt6fy+18R98iqvBFiKi5njo50Nr+yTHQuSTfWF
X6I2uhYNML6/aC8EBYFbTjVuJXyIOrM7CqnP77SbavA=="
}'
```

۲-۴-۲ استعلام با رسید یکنای دریافت صورتحساب (Inquiry_by_reference_number):

• نمونه ارسال درخواست CURL:

```
curl --location --request POST
'https://tp.tax.gov.ir/req/api/tsp/sync/INQUIRY_BY_REFERENCE_NUMBER' \
--header 'requestTraceId: 1655186644886' \
--header 'timestamp: 1655186644886' \
--header 'Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJjbGllbnRUeXB1IjoiVEFNQIiwidG9rZW5JZCI6IjZlODlhZDQ3LTBl
ZjQtNDRmNC05YWZkLWl5MjdlNDM1ZmI2NyIsInBlcm1pc3Npb25zIjpbInRzcC5hc3luYy5mYXN0
LWVucXVldWUiLCJ0c3AuYXN5bmMubm9ybWVsLWVucXVldWUiLCJ0c3Auc3luYyJdLCJwYWNrZXRUeX
BlcyI6IjYwYjHRVRFURNPtK9NSUNfQ09ERV9JTkJZPUk1BVElPTiIsIk10UUVVJU11fQ11fVE1NRSIsIk
dFVF9TRVJWRVJfSU5GT1JNQVRJT04iLCJjJT1FVSVJZXR0ZXR1VJRCIsIk10UUVVJU11fQ11fVUkVGRVJF
```

```

TkNFX05VTUJFUiiIsIkdFVF9UT0tFTiIsIkdFVF9GSVNDQUxfsU5GT1JNQVRJT04iLCJTTlZPSUNFL
lYwMSIsIk10UVVJU11fQ11fVE1NRV9SQU5HRISIsIkdFVF9TRVJWSUNFX1NUVUZGX0xJU1QixSWiaX
NzIjoiVEFYIE9yZ2FuaXphdGlvbiIsImlkIjoidGVzdC10c3AtaWQtMSIsImV4cCI6MTY1NTIwMDM
40CwiY3JlYXRIRGF0ZSI6MTY1NTE4NTk4ODQ5Mn0.SF06IpHsdSEKHDC0V1X7oqgVITzy5S3kseHS
HSbdrfwiaYxDt1mMn541TV8zP-HowhBs8u1fjs_S81kiZON4FA' \
--header 'Content-Type: application/json' \
--data-raw '{
  "time": 1,
  "packet": {
    "uid": null,
    "packetType": "INQUIRY_BY_REFERENCE_NUMBER",
    "retry": false,
    "data": {
      "referenceNumber":
        ["04af9b37-07e4-4019-88c2-efeea844552f", "99fab38b-b32f-49cb-89d8-
        71e52cae2d91", "6c2983cb-0fe4-4da4-b93f-2e30e9652631"]
    },
    "encryptionKeyId": "",
    "symmetricKey": "",
    "iv": "",
    "fiscalId": "AA56CD",
    "dataSignature": ""
  },
  "signature":
    "MMY9CYojEiPEYg1I0gNbahYLJfST7VEEYA7bXr7/ZTHjvYMEoUeFQU9EcaN2sIhx/833abKw7FD0
    cHeICnEBCWngc0WowS1ZScfWlviW8hrRQ1AAZjaZcPw0JUXLgkM2rdUDPTBy8ENUb0GmGvDajc00F
    Nb03GAtRD97szK8Na56qSDsnG7uDpqsX2r+xI0JtUKxJFJyL1i57u2wZbwUCw2uN70cd0XDD08oLZ
    I2CQxvwu/TV+vzaFOPq1TYtLk54H82ShFtXtaqbHnt7RTtX70a0s0P16SYxDaMfrr0EuV0p3FI51F
    wz3TZzYF00AVaSExv95UT5fRXKSOZDWhzPw=="
}'

```

۲-۳ دریافت خطاهای بسته‌های ارسالی غیرهمگام با استفاده از زمان (INQUIRY_BY_TIME):

• نمونه CURL:

```

curl --location --request POST
'https://tp.tax.gov.ir/req/api/tsp/sync/INQUIRY_BY_TIME' \
--header 'requestTraceId: 1655186330848' \
--header 'timestamp: 1655186330848' \
--header 'Authorization: Bearer
eyJhbGciOiJIUzUxMiJ9.eyJjbGllbnRUeXB1IjoiVFNQIiwidG9rZW5JZCI6IjZlODlhZDQ3LTB1
ZjQtNDRmNC05YWZkLWI5MjdlNDM1ZmI2NyIsInBlcm1pc3Npb25zIjpbInRzcC5hc3luYy5mYXN0L
wVucXVldWUiLCJ0c3AuYXN5bmMubm9ybWFsLWVucXVldWUiLCJ0c3Auc3luYyJdLCJwYWNrZXRUEX
BlcyI6WyJHRVRFRUNPTk9NSUNfQ09ERV9JTkZPUk1BVE1PTiIsIk10UVVJU11fQ11fVE1NRSIsIkd
FVF9TRVJWRVJfSU5GT1JNQVRJT04iLCJTTlFVSVJZX0JZX1VJRCIsIk10UVVJU11fQ11fUkVGRVJF

```

```
TkNFX05VTUJFUiiIsIkdFVF9UT0tFTiIsIkdFVF9GSVNDQUxfSU5GT1JNQVRJT04iLCJjTlZPSUNFL
lYwMSIsIk1OUVVJU1lfQ1lfVE1NRV9SQU5HRSIkdfVF9TRVJWSUNFX1NUVUZGX0xJU1QiXSwiaX
NzIjoiveFEYIE9yZ2FuaXphdGlvbiIsImlkIjoidGVzdC10c3AtaWQtMSIsImV4cCI6MTY1NTIwMDM
4OCwiY3JlYXRIRGF0ZSI6MTY1NTE4NTk4ODQ5Mn0.SF06IpHsdSEKHDC0V1X7oqgVITzy5S3kseHS
HSbdrfwiaYxDT1mMn541TV8zP-HowhBs8u1fjs_S81kiZON4FA' \
--header 'Content-Type: application/json' \
--data-raw '{
  "time": 1,
  "packet": {
    "uid": null,
    "packetType": "INQUIRY_BY_TIME",
    "retry": false,
    "data": {
      "time" :
        14010321
    },
    "encryptionKeyId": "",
    "symmetricKey": "",
    "iv": "",
    "fiscalId": "",
    "dataSignature":""
  },
  "signature":
    "e1HDykQjZBzgM9NIMSEVR+dYfDcAbowWF00vEzI31WRuBwMVmmmYkXg6b4q6oIj+78Cgwd106Jo4
5zuaH1eNSxVc67xr7hagpnyvnVQYt2ot3Y5Rk+MJ0BkyfE06qv45yzV2kwe5CkfCAH2ccvFnnkEGd
o15CoaAyJk51hWNTppGm0dXAwoEoUE2gjDRZqtRsgzMOmum5ep7GoPQ/8WildwNgxuVRLaWiQNmZs
EuBDVLgJsY7xFMGczFCyZt1NwZwV1FVTDZVmn8XNDC1u7e0IRX/krnF932EAxWiWG5zidyr/geXyz
gpmFevQQbe10eedCuLcFVT+GrNGfJUuzakw=="
}'
```



۴-۴-۲ دریافت خطاهای بسته‌های ارسالی غیرهمگام با استفاده از بازه زمانی (INQUIRY_BY_TIME_RANGE)

• نمونه CURL:


```

"uid": null,
"packetType": "INQUIRY_RESULT",
"data": [
  {
    "referenceNumber": "967072eb-203e-428e-b9bb-6d2efdb9d356",
    "uid": "8a00f17a-bd35-46bc-ae52-3f61fab868c2",
    "status": "SUCCESS",
    "data": {
      "confirmationReferenceId": "d4c0e7e6-d42e-11ec-9d64-0242ac120002",
      "taxResult": "SUCCESS"
    },
    "packetType": "RECEIVE_INVOICE_CONFIRM",
    "fiscalId": "SAU5BC"
  }
],
"encryptionKeyId": null,
"symmetricKey": null,
"iv": null
}

```

نمونه پاسخ درخواست های استعلام در صورت رخ دادن خطا:

```

{
  "uid": null,
  "packetType": "INQUIRY_RESULT",
  "data": [
    {
      "referenceNumber": "6df7b185-5254-4f58-b3e6-61169b5d5929",
      "uid": "3b33584c-331e-4fbc-97ea-8d294a2009db",
      "status": "FAILED",
      "data": {
        "confirmationReferenceId": null,
        "taxResult": "memory-id.is.null"
      },
      "packetType": "ERROR",
      "fiscalId": null
    }
  ],
  "encryptionKeyId": null,
  "symmetricKey": null,
  "iv": null
}

```

۲-۵- دریافت اطلاعات سرور (GET_SERVER_INFORMATION)

- نمونه CURL:

```
curl --location --request POST
'https://tp.tax.gov.ir/req/api/tsp/sync/GET_SERVER_INFORMATION' \
--header 'requestTraceId: 1654938179880' \
--header 'timestamp: 1654938179880' \
--header 'Content-Type: application/json' \
--data-raw '{
  "time": 1,
  "packet": {
    "uid": null,
    "packetType": "GET_SERVER_INFORMATION",
    "retry": false,
    "data": null,
    "encryptionKeyId": "",
    "symmetricKey": "",
    "iv": "",
    "fiscalId": "",
    "dataSignature": ""
  }
}'
```

- نمونه پاسخ درخواست:

```
{
  "signature": null,
  "signatureKeyId": null,
  "timestamp": 1655184692934,
  "result": {
    "uid": null,
    "packetType": "SERVER_INFORMATION",
    "data": {
      "serverTime": 1655184692934,
      "publicKeys": [
        {
          "key":
"MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICGKCAgEAXdzREOEfk3vBQogDPGTMqdDQ7t0oDhuK
MZkA+Wm1lhzzjhAGfSU0uDvOKRoUEQwP8oUcXRmYzcvCUGcfoRT5iz7HbovqH+bIeJwT4rmLmFcbf
Pke+E3DLUX0tIZifEXrKXWgSVPkRnhMgym6UiAtnzwA1rmKstJoWpk9Nv34CYgTk8DKQN5jQJqb9L
/Ng0z0EEtI3zA424tsd9zv/kP4/SaSnbbnj0evqsZ29X6aBypvnTnwH9t3gbWM4I9eAVQhPYC1awH
TqvdaZ/O/feqfm06QBFnCGl+CBdjLs30xQSLsPICjn1V1jMzoTZnAabWP6FRzzj6C2sXw9a/Ww1Xr
Kn3gldZ7Ctv6Jso72cEeCeUI1tzHMDJPU3Qy12RQzaXujpMhCz1Dva47RvqiumpTnyK9HFFIdhgou
pFkxT14XLD16S55MF6HuQvo/RHSbBJ93FQ+2/x/Q2MNGB3BX0jNwM2pj3ojbDv3pj9CHzvaYQUYM
1y0cFmIJqJ72uvVf9Jx9iT0baNNF6p152ADmh85GTAH1hz+4pR/E9IAXUI1/YiUneYu0G4tiDY4ZX
```

```

ykYNknNfhSgxmn/gPHT+7kL31nyxgjiEEhK0B0vagWvdRCNJSNGWpLt1q4F1CWtAnPI5ctiFgq925
e+sySjNaORCoHraBXNEwyiHT2hu5ZipIW2cCAwEAAQ==",
      "id": "6a2bcd88-a871-4245-a393-2843eafe6e02",
      "algorithm": "RSA",
      "purpose": 1
    }
  ]
},
"encryptionKeyId": null,
"symmetricKey": null,
"iv": null
}
}

```

۲-۶ دریافت لیست کامل شناسه کالا/خدمات و نرخ مالیاتی (GET_SERVICE_STUFF_LIST)

• نمونه CURL:

```

curl --location --request POST 'https://tp.tax.gov.ir/req/api/tsp/sync/
GET_SERVICE_STUFF_LIST \
--header 'requestTraceId: 1654521784527' \
--header 'timestamp: 1654521784527' \
--header 'Content-Type: application/json' \
--data-raw '{
  "time": 1,
  "packet": {
    "uid": null,
    "packetType": "GET_SERVICE_STUFF_LIST",
    "retry": false,
    "data": {
      "page" : 1,
"size" : 10
    },
    "encryptionKeyId": "",
    "symmetricKey": "",
    "iv": "",
    "fiscalId": "",
    "dataSignature": ""
  }
}'

```

• نمونه پاسخ:

```

{
  "signature": null,

```

```

"signatureKeyId": null,
"timestamp": 1655190910633,
"result": {
  "uid": null,
  "packetType": "SERVICE_STUFF_LIST",
  "data": {
    "result": [
      {
        "tax": 9,
        "itemId": "1"
      }
    ],
    "pagination": {
      "size": 10,
      "page": 1,
      "total": 1
    }
  },
  "encryptionKeyId": null,
  "symmetricKey": null,
  "iv": null
}
}

```

۲-۷ استعلام اطلاعات شماره اقتصادی (GET_ECONOMIC_CODE_INFORMATION):

نمونه CURL:

```

curl --location --request POST
'https://tp.tax.gov.ir/req/api/tsp/sync/GET_ECONOMIC_CODE_INFORMATION' \
--header 'requestTraceId: 1654521302712' \
--header 'timestamp: 1654521302712' \
--header 'Content-Type: application/json' \
--data-raw '{
  "time": 1,
  "packet": {
    "uid": null,
    "packetType": "GET_ECONOMIC_CODE_INFORMATION",
    "retry": false,
    "data": {
      "economicCode": "12345678911234"
    }
  },
}'

```

```

    "encryptionKeyId": "",
    "symmetricKey": "",
    "iv": "",
    "fiscalId": "",
    "dataSignature": ""
  }
}'

```

• نمونه پاسخ:

```

{
  "signature": null,
  "signatureKeyId": null,
  "timestamp": 1655191021181,
  "result": {
    "uid": null,
    "packetType": "ECONOMIC_CODE_INFORMATION",
    "data": {
      "nameTrade": "پیشخوان دولت",
      "taxpayerStatus": "فعال",
      "taxpayerType": "حقوقی",
      "postalcodeTaxpayer": "",
      "addressTaxpayer": "تهران"
    },
    "encryptionKeyId": null,
    "symmetricKey": null,
    "iv": null
  }
}

```