

روش جدید اتصال به درگاه چند  
پرداختی شرکت پرداخت الکترونیک  
پاسارگاد- تسهیم از طریق سویچ

مستندات فنی



پرداخت الکترونیک  
**پاسارگاد**

واحد پایانه های اینترنتی

## واحد پایانه های اینترنتی شرکت پرداخت الکترونیک پاسارگاد

روش جدید اتصال به درگاه چند پرداختی شرکت پرداخت الکترونیک پاسارگاد- تسهیم از طریق سویچ



صفحه ۱

PEP IPG REST MultiPayment.13971124.Ver3.00

۱۳۹۷/۱۱/۲۴

### فهرست مطالب

۲	مقدمه.....
۳	۱. تعاریف.....
۳	۱-۱. تعاریف مرتبط با خریدار.....
۳	۱-۲. تعاریف مرتبط با فروشنده.....
۵	۱-۳. تعاریف مرتبط با درگاه پرداخت اینترنتی و عملیات مالی.....
۷	۲. مراحل کلی فرآیند خرید.....
۸	۳. دریافت توکن پرداخت.....
۱۰	۴. ارجاع خریدار به درگاه پرداخت پپ.....
۱۱	۵. استعلام نتیجه تراکنش.....
۱۴	۶. تایید خرید.....
۱۶	۷. برگشت از خرید.....
۱۷	۸. استفاده از swagger جهت تست سرویس های API.....

## مقدمه

خرید اینترنتی یکی از تراکنش‌های کارتی است که در مرکز شاپرک نیز جزو تراکنش‌های مجاز محسوب می‌شود. در این مستند گام‌های لازم برای ایجاد بستر پرداخت الکترونیکی در سمت وب‌سایت پذیرنده شرح داده شده است. این خدمت پذیرندگان را قادر می‌سازد تا از طریق درگاه پرداخت اینترنتی شرکت پرداخت الکترونیک پاسارگاد به خریداران خود سرویس ارائه دهد. لازم به ذکر است که این مستند علاوه بر شرح روال خرید به بررسی چگونگی تسویه مبلغ پرداختی و واریز این مبالغ به حساب‌های جداگانه‌ی پذیرنده می‌پردازد. این نسخه از سرویس در مقایسه با نسخه‌های پیشین تفاوت‌های بسیاری از لحاظ معماری و عملکرد را دارا می‌باشد، به گونه‌ای که تمامی متدهای ثبت درخواست خرید، استعلام وضعیت خرید، برگشت و تایید خرید در قالب RESTful API ارائه شده‌اند. علاوه بر این کلیه پارامترهای ورودی و خروجی وب‌سرویس از نوع JSON بوده و در زمان هدایت خریدار از وب‌سایت پذیرنده به درگاه پرداخت تنها می‌بایست مقدار توکن به درگاه پرداخت ارسال گردد. از این رو حجم داده‌های ارسالی به درگاه پرداخت کاهش قابل توجهی پیدا کرده‌است.

## ۱. تعاریف

### ۱-۱ تعاریف مرتبط با خریدار

- **خریدار:** هویتی است که توسط یکی از انواع کارت‌های بانکی عضو شبکه شتاب و با مراجعه به وب سایت مورد نظر خود تقاضای خرید کالا یا خدمات را دارد.
- **خرید چند پرداختی:** منظور از خرید در این مستند، تراکنش خریدی است که در آن فروشنده می تواند با ارسال یک دستور پرداخت هنگام خرید، مبلغ تراکنش را به چندین شبای از پیش تعریف شده، واریز نماید.

### ۱-۲ تعاریف مرتبط با پذیرنده

- **پذیرنده:** هویتی است که با آماده‌سازی بستر پرداخت اینترنتی، اقدام به فروش کالا و خدمات از طریق وب سایت خود می‌نماید.
- **شماره شناسائی پذیرنده (MerchantCode):** کدی است که توسط شرکت پرداخت الکترونیک به پذیرنده اختصاص می‌یابد و در حین انجام تراکنش برای شناسایی پذیرنده از آن استفاده می‌گردد.
- **شماره شناسائی ترمینال (TerminalCode):** کدی است که توسط شرکت پرداخت الکترونیک به پذیرنده اختصاص می‌یابد و در حین انجام تراکنش از آن استفاده می‌گردد.
- **کلید خصوصی پذیرنده (PrivateKey):** کلیدی است که پذیرنده برای احراز هویت از آن استفاده می‌کند و تمامی داده‌های ارسالی خود به شرکت پرداخت الکترونیک را با آن کلید، امضای دیجیتال می‌کند.
- **کلید عمومی پذیرنده (PublicKey):** کلیدی است که درگاه پرداخت اینترنتی جهت تایید امضای دیجیتال فروشگاه از آن استفاده می‌کند.
- **سپرده فروشنده:** شماره شبای پذیرنده می باشد که جهت انجام عمل تسویه حساب به شرکت پرداخت الکترونیک پاسارگاد اعلام می شود.
- **مبلغ فاکتور (Amount):** مبلغی می‌باشد که پذیرنده می‌خواهد از خریدار دریافت نماید.
- **شماره فاکتور (InvoiceNumber):** هر خرید از پذیرنده باید دارای شماره فاکتور خاص خود باشد.
- **تاریخ فاکتور (InvoiceDate):** تاریخ فاکتور خرید است و فرمت آن به انتخاب فروشگاه می‌باشد (لازم به ذکر است که تاریخ و شماره فاکتور، باید به‌گونه‌ای تخصیص داده شوند که از ترکیب آنها شناسه یکتایی بدست آید تا همیشه بتوان برای شناسایی یک تراکنش خرید از آن استفاده کرد).

- **امضای دیجیتال (DigitalSignature):** امضای دیجیتال روشی مبتنی بر الگوریتم های رمزنگاری نامتقارن می باشد که به کمک آن می توان اطمینان حاصل کرد که داده های ارسالی از جانب فروشگاه مشخصی ارسال شده است.
- **آدرس بازگشت (RedirectAddress):** آدرس صفحه ای در سایت پذیرنده است که خریدار پس از انجام عملیات خرید به آن فرستاده می شود.
- **Timestamp:** زمان ارسال داده به درگاه پرداخت را Timestamp می گویند که فرمت آن به شکل "YYYY/MM/DD HH:MM:SS" بوده و به تاریخ میلادی ارسال می گردد. اگر هرکدام از عددهای ماه، روز، ساعت، دقیقه یا ثانیه یک رقمی باشد با قراردادن یک صفر در سمت چپ آن باید عدد دو رقمی تولید شده و برای بانک ارسال شود. نکته ی مهم در اینجا این است که مقداری که در فیلد Timestamp قرار می گیرد باید دقیقاً با مقداری که تحت همین عنوان در امضای دیجیتال قرار می گیرد یکی باشد، همچنین هیچ دو درخواستی، نمی توانند دارای Timestamp یکسان باشند.
- **تلفن همراه (Mobile):** شماره تلفن همراه خریدار است که توسط فروشگاه برای درگاه پرداخت ارسال می گردد. در صورت ارسال این فیلد توسط فروشگاه، درگاه پرداخت، شماره کارت های ثبت شده کاربر در سامانه پیوند را نمایش می دهد و در غیراینصورت هیچ شماره کارتی نمایش داده نمی شود. همچنین در صورت ارسال این فیلد، کاربر می تواند اطلاعاتی از قبیل شماره کارت و تاریخ انقضای کارت خود را در درگاه پرداخت جهت سهولت انجام خرید در مراجعات بعدی ذخیره نماید.  
نکته: قالب صحیح ارسال شماره تلفن همراه به صورت "۹۱۲۴۴۴۲۲۱۱" می باشد.
- **پست الکترونیک (Email):** آدرس پست الکترونیک خریدار است که می تواند توسط وب سایت فروشگاه به درگاه پرداخت ارسال شود. در صورت ارسال این فیلد توسط فروشگاه، فیلد ایمیل در درگاه پرداخت با آدرس ارسالی پر می شود.
- **نام پذیرنده (MerchantName):** نام پذیرنده است که می تواند توسط وب سایت فروشگاه به درگاه پرداخت ارسال شود. در صورت ارسال این فیلد توسط فروشگاه، فیلد نام فروشگاه در درگاه پرداخت با نام ارسالی پر می شود، در غیراینصورت نامی که قبلاً در هنگام ثبت نام فروشگاه در شرکت پرداخت الکترونیک

پاسارگاد ثبت شده، نمایش داده می‌شود. لازم به ذکر است در صورتی که پذیرنده می‌خواهد از این قابلیت استفاده نماید، می‌بایست درخواست فعالسازی آن را به شرکت پرداخت الکترونیک پاسارگاد بدهد.

- اطلاعات چندپرداختی (MultiPaymentData): یک xml از لیست ریزپرداخت‌ها به صورت زیر می‌باشد که به رشته‌ای با فرمت base64String تبدیل می‌شود.

```
<item>
  <iban>IR310600780901000423591771</iban>
  <type>0</type>
  <value>12000</value>
</item>
```

**iban** : شماره شبا می‌باشد.

**type** : نوع محاسبه‌ی مبلغ ریزپرداخت‌ها.

- در صورتی که پارامتر **type** برابر با صفر باشد **value** با مبلغ مقدردهی می‌شود.
- در صورتی که پارامتر **type** برابر با یک باشد **value** براساس درصد بوده که عدد مربوطه می‌بایست بزرگتر از صفر، کوچکتر مساوی ۱۰۰ و همچنین می‌تواند عدد اعشاری باشد.

**نکته:** هر آیتم نمایانگر یک ریزپرداخت می‌باشد و می‌توان حداکثر ۱۰ آیتم در یک تراکنش چند پرداختی قرار داد.  
**نکته:** مقدار درصد ارسالی باید به صورت اعشاری باشد. به طور مثال عدد ۵ درصد به صورت ۵,۰۰ ارسال می‌شود.  
**نکته:** جمع مبالغ آیتم‌ها در یک تراکنش چندپرداختی نباید از مبلغ اصلی تراکنش بیشتر باشد و در صورت وارد کردن مقدار براساس درصد، مجموع نباید بیشتر از ۱۰۰ و از مبلغ اصلی تراکنش بیشتر باشد. در صورتی که جمع مبالغ از مبلغ اصلی تراکنش بیشتر باشد تراکنش ناموفق و در صورتی که کمتر باشد مابه تفاوت آن به شبای اصلی تخصیص داده خواهد شد.

**نکته:** در صورتی که به طور همزمان مبلغ و درصد مقدار داشته باشد ، مقدار فیلد مبلغ مورد استفاده قرار خواهد گرفت.

**نکته:** مقداردهی فیلد Value اجباری است.

### ۱-۳ تعاریف مرتبط با درگاه پرداخت و عملیات مالی

- درگاه پرداخت اینترنتی شرکت پرداخت الکترونیک پاسارگاد (Internet Payment Gateway): سایتی است متعلق به شرکت پرداخت الکترونیک پاسارگاد که در آن خریدار پس از انتخاب موارد مورد خرید خود

## واحد پایانه های اینترنتی شرکت پرداخت الکترونیک پاسارگاد

روش جدید اتصال به درگاه چند پرداختی شرکت پرداخت الکترونیک پاسارگاد- تسهیم از طریق سوییچ



شرکت پرداخت الکترونیک  
بانک پاسارگاد

صفحه 6

PEP IPG REST MultiPayment.13971124.Ver3.00

۱۳۹۷/۱۱/۲۴

در سایت پذیرنده ، به آنجا هدایت می شود و در آنجا مشخصات کارت و رمز خود را وارد می نماید، سپس درگاه پرداخت تراکنش مورد نظر خریدار را انجام داده و در نهایت پذیرنده را از نتیجه آن آگاه می سازد.  
نکته: شرکت پرداخت الکترونیک پاسارگاد ازین پس با نام پپ (Pep) در این مستند ذکر خواهد شد.

- **نوع تراکنش (Action):** نشان دهندهی نوع عملیات مالی مورد نظر می باشد که در این سیستم کد ۱۰۰۳ جهت عملیات خرید می بایست ارسال گردد.
- **شماره رهگیری (TransactionReferenceID):** شماره ای است که درگاه پپ پس از موفقیت آمیز بودن تراکنش به سایت پذیرنده ارسال می کند و به وسیله آن پذیرنده می تواند از موفقیت آمیز بودن تراکنش اطلاع یابد.
- **تسویه حساب:** واریز وجوه دریافتی از خریدار به سپرده پذیرنده توسط پپ می باشد که در صورت موفق بودن تراکنش خرید پس از کسر کارمزد انجام می شود.
- **Token:** مقداری است که در پاسخ فراخوانی سرویس GetToken به پذیرنده برگردانده می شود و جهت آغاز فرایند خرید پذیرنده می بایست خریدار خود را به همراه توکن دریافتی به درگاه پپ پرداخت هدایت نماید.

## ۲. مراحل کلی فرآیند خرید

- ۲-۱ ورود مشتری به سایت پذیرنده و تشکیل سبد خرید یا انتخاب خدمات مورد نظر.
- ۲-۲ فراخوانی متد GetToken و دریافت توکن توسط پذیرنده.
- ۲-۳ هدایت مشتری به درگاه پپ به همراه توکن دریافتی.
- ۲-۴ تکمیل اطلاعات کارت توسط مشتری و انجام مرحله‌ی پرداخت وجه.
- ۲-۵ هدایت مشتری به سایت پذیرنده پس از انجام عملیات پرداخت توسط مشتری.
- ۲-۶ ادامه روند عملیات خرید مشتری در سایت پذیرنده پس از دریافت نتیجه تراکنش از طریق وبسرویس.
- ۲-۷ نهایی کردن تراکنش خرید پس از ارائه‌ی خدمات به خریدار. پذیرنده می‌بایست با استفاده از وبسرویس تایید خرید تراکنش مربوطه را نهایی کند. لازم به ذکر است در صورت عدم تایید، مبلغ تراکنش پس از مهلت تعیین شده به حساب مشتری عودت پیدا خواهد کرد.
- ۲-۸ در هر صورت، اگر پذیرنده قصد ابطال تراکنش را داشته باشد می‌تواند تا ۲ ساعت بعد از تراکنش به وسیله وبسرویس ارائه شده اقدام به برگشت خرید نماید.

### ۳. دریافت توکن پرداخت

خریدار با مراجعه به وبسایت پذیرنده و انتخاب کالا یا خدمات مورد نیاز، آماده پرداخت مبلغ فاکتور می‌شود. سایت پذیرنده می‌بایست اطلاعات مربوط به تراکنش خرید را با PrivateKey خود امضا کرده و از طریق آدرس <https://pep.shaparak.ir/Api/v1/Payment/GetToken> به وبسرویس پپ ارسال نماید. در صورتی که اطلاعات ارسالی از جانب پذیرنده معتبر باشد توکن تولید شده به پذیرنده برگردانده خواهد شد. پذیرنده در مرحله بعد می‌تواند با توکن دریافتی، مشتری خود را به درگاه پپ هدایت نماید. جزئیات فراخوانی این متد در جدول زیر شرح داده شده است.

آدرس		
<a href="https://pep.shaparak.ir/Api/v1/Payment/GetToken">https://pep.shaparak.ir/Api/v1/Payment/GetToken</a>		
متد		
POST		
نام فیلد (موارد ستاره‌دار ضروری می‌باشند)	نوع فیلد	توضیحات
Content-Type *	String	فرمت محتوی درخواست Application/json
Sign *	String	امضای دیجیتال پارامترهای ورودی (پیوست ۲)
InvoiceNumber *	String	شماره فاکتور
InvoiceDate *	String	تاریخ فاکتور
TerminalCode *	Int	کد ترمینال
MerchantCode *	Int	کد پذیرنده
Amount *	Decimal	مبلغ تراکنش
RedirectAddress *	String	آدرس بازگشت به سایت پذیرنده
Timestamp *	String	زمان ارسال تراکنش با فرمت 2018/09/18 15:15:13
Action *	Int	خرید ۱۰۰۳
Mobile	String	شماره موبایل خریدار
Email	String	ایمیل خریدار
MerchantName	String	در صورت داشتن مجوز ارسال شود
MultiPaymentData *	String	جزئیات ریزپرداخت‌ها با فرمت base64String
IsSuccess	Bool	False   True
Message	String	پیغام
Token	String	توکن تولید شده جهت عملیات پرداخت

## واحد پایانه های اینترنتی شرکت پرداخت الکترونیک پاسارگاد

روش جدید اتصال به درگاه چند پرداختی شرکت پرداخت الکترونیک پاسارگاد- تسهیم از طریق سوییچ



شرکت پرداخت الکترونیک  
پاسارگاد

صفحه ۹

PEP IPG REST MultiPayment.13971124.Ver3.00

۱۳۹۷/۱۱/۲۴

خروجی	ورودی	نمونه Json
موفق		
<pre>{   "IsSuccess": true,   "Message": "عملیات با موفقیت انجام شد",   "Token": "02302dasd15a1f121fasd2asda" }</pre>		
ناموفق		
<pre>{   "IsSuccess": false,   "Message": "تراکنش ارسالی معتبر نیست" }</pre>		
موفق: 200 Ok		کد پاسخ HTTP

## ۴. ارجاع خریدار به درگاه پرداخت پپ

در صورتی که دریافت توکن با موفقیت انجام شد، سایت پذیرنده می‌بایست خریدار را همراه با توکن دریافتی به درگاه پرداخت هدایت کند. پذیرنده می‌تواند با یکی از دو روش زیر خریدار را به درگاه پرداخت هدایت نماید.

### ۴-۱ ارسال خریدار به درگاه با استفاده از متد Get

پس از دریافت توکن، پذیرنده می‌تواند خریدار را با آدرس <https://pep.shaparak.ir/payment.aspx?n=Token> به درگاه پرداخت پپ هدایت نماید. لازم به ذکر است که در آدرس ذکر شده به جای Token می‌بایست مقدار توکن دریافتی (در مرحله دریافت توکن پرداخت) جایگذاری گردد.

### ۴-۲ ارسال خریدار به درگاه با استفاده از متد Post

در صورتی که دریافت توکن با موفقیت انجام شد، سایت پذیرنده می‌بایست توکن دریافتی را با متد HTTP POST به سایت پپ <https://pep.shaparak.ir/payment.aspx> ارسال نماید. فرم ارسالی از سایت پذیرنده می‌بایست شامل فیلدی با مقدار توکن دریافتی و با نام Token باشد. نمونه کد HTML مورد نیاز در پیوست ۴ آورده شده است. مشتری پس از هدایت شدن به درگاه پپ با وارد کردن شماره کارت (PAN)، کلمه عبور اینترنتی (PIN2)، کد اعتبارسنجی دوم (CVV2) و تاریخ انقضای کارت (Expiration Date) اقدام به پرداخت مبلغ مورد نظر پذیرنده می‌نماید. در این مرحله تراکنش توسط درگاه پپ پردازش گردیده و عملیات لازم در مرکز شاپرک و بانک صادرکننده کارت انجام می‌پذیرد.

وب سایت پپ پس از انجام تراکنش، مشتری را به آدرسی که در هنگام دریافت توکن پذیرنده در فیلد `redirectAddress` قرار داده است هدایت می‌نماید و در `QueryString` آن مقادیر زیر را قرار می‌دهد.

- InvoiceNumber (در فیلد iN)
- InvoiceDate (در فیلد iD)
- TransactionReferenceID (در فیلد tref)

## ۵. استعلام نتیجه تراکنش

سایت پذیرنده در این گام می تواند با فراخوانی متد CheckTransactionResult در وب سرویس پپ از نتیجه عملیات خرید باخبر شود. متد CheckTransactionResult به دو روش زیر قابل فراخوانی می باشد.

### ۵-۱ در صورت دریافت نتیجه تراکنش

در صورتی که سایت پذیرنده مقادیر ارسالی از درگاه پرداخت الکترونیک پاسارگاد به سایت پذیرنده را دریافت نموده باشد می تواند تنها با تکمیل فیلد TransactionReferenceID، نتیجه تراکنش خریدار خود را دریافت نماید. جزئیات فراخوانی این متد در جدول زیر شرح داده شده است.

### ۵-۲ در صورت عدم دریافت نتیجه تراکنش

در صورتی که سایت پذیرنده به هر دلیلی در مرحله انتقال از درگاه به سایت پذیرنده موفق به دریافت TransactionReferenceID نشود می تواند با مقداردهی فیلدهای شماره فاکتور، تاریخ فاکتور، شماره شناسایی پذیرنده و شماره شناسایی ترمینال از نتیجه تراکنش خریدار خود باخبر شود. سایت پپ پس از تطبیق دادن پارامترهای ارسالی با فاکتور اصلی، نتیجه تراکنش را خوانده و اقدام مقتضی را انجام می دهد. جزئیات فراخوانی این متد در جدول زیر شرح داده شده است.

نکته: لازم به ذکر است که پذیرنده می بایست نتیجه تراکنش را چک کرده و از موفق بودن تراکنش اطمینان حاصل کند و به صرف دریافت TransactionReferenceID از درگاه، تراکنش را موفقیت آمیز تلقی نکند.

## واحد پایانه های اینترنتی شرکت پرداخت الکترونیک پاسارگاد

روش جدید اتصال به درگاه چند پرداختی شرکت پرداخت الکترونیک پاسارگاد- تسهیم از طریق سوییچ



صفحه ۱۲

PEP IPG REST MultiPayment.13971124.Ver3.00

۱۳۹۷/۱۱/۲۴

https://pep.shaparak.ir/Api/v1/Payment/CheckTransactionResult			آدرس
POST			متد
توضیحات	نوع فیلد	نام فیلد	
فرمت محتوی درخواست Application/json	String	Content-Type	
شماره فاکتور (در حالت ۵-۲ تکمیل گردد)	String	InvoiceNumber	
تاریخ فاکتور (در حالت ۵-۲ تکمیل گردد)	String	InvoiceDate	
کد ترمینال (در حالت ۵-۲ تکمیل گردد)	Int	TerminalCode	
کد مشتری (در حالت ۵-۲ تکمیل گردد)	Int	MerchantCode	
شماره ارجاع داخلی موجود در QueryString در زمان هدایت خریدار از صفحه درگاه پرداخت به RedirectAddress اعلام شده توسط پذیرنده پس از انجام عملیات پرداخت. (در حالت ۵-۱ تکمیل گردد)	String	TransactionReferenceID	
False   True	Bool	IsSuccess	
پیغام	String	Message	
شماره ارجاع	long	ReferenceNumber	
شماره پیگیری	int	TraceNumber	
تاریخ تراکنش	String	TransactionDate	
خرید ۱۰۰۳	String	Action	
شماره ارجاع داخلی	String	TransactionReferenceID	
شماره فاکتور	String	InvoiceNumber	
تاریخ فاکتور	String	InvoiceDate	
کد پذیرنده	Int	MerchantCode	
کد ترمینال	Int	TerminalCode	
مبلغ تراکنش	decimal	Amount	
خروجی			ورودی
موفق			

واحد پایانه های اینترنتی شرکت پرداخت الکترونیک پاسارگاد



روش جدید اتصال به درگاه چند پرداختی شرکت پرداخت الکترونیک پاسارگاد- تسهیم از طریق سوییچ

صفحه ۱۳

PEP IPG REST MultiPayment.13971124.Ver3.00

۱۳۹۷/۱۱/۲۴

<pre>{   "TraceNumber": 13,   "ReferenceNumber": 100200300400500,   "TransactionDate": "2019/01/29 18:07:29",   "Action": "1003",   "TransactionReferencID": "636843820118990203",   "InvoiceNumber": "80",   "InvoiceDate": "2019/01/29 18:06:43",   "MerchantCode": 550166,   "TerminalCode": 550363,   "Amount": 10000,   "IsSuccess": true,   "Message": "عملیات به اتمام رسید" }</pre>	<pre>{   "InvoiceNumber": "123456",   "InvoiceDate": "1349/04/04",   "TerminalCode": "1",   "MerchantCode": "1" } یا {   "TransactionReferencID": "324324234" }</pre>	
ناموفق		
<pre>{   "IsSuccess": false,   "Message": "تراکنش ارسالی معتبر نیست" }</pre>		
موفق: 200 Ok		کد پاسخ HTTP

## ۶. تایید خرید

در صورتی که عملیات خرید با موفقیت انجام شده باشد، درگاه پپ مدت زمان مشخصی منتظر می ماند تا خرید انجام شده توسط فروشنده تایید شود. در صورتی که خرید طی این مدت زمان توسط پذیرنده تایید نشود درگاه پپ به صورت خودکار آن را برگشت زده و پول به حساب خریدار باز می گردد. لازم به ذکر است که مدت زمانی که بانک برای تایید خرید از سمت پذیرنده منتظر می ماند طبق توافق پپ و پذیرنده می باشد.

در نتیجه پذیرنده پس از دریافت نتیجه تراکنش می بایست از طریق فراخوانی متد VerifyPayment در وب سرویس پپ اقدام به تایید خرید خریدار خود نماید. توجه شود که برای تایید خرید، پذیرنده باید شماره فاکتور و تاریخ

## واحد پایانه های اینترنتی شرکت پرداخت الکترونیک پاسارگاد

روش جدید اتصال به درگاه چند پرداختی شرکت پرداخت الکترونیک پاسارگاد- تسهیم از طریق سویچ



صفحه ۱۵

PEP IPG REST MultiPayment.13971124.Ver3.00

۱۳۹۷/۱۱/۲۴

فاکتور تراکنش خرید (تراکنش اصلی) را ارسال کند ولی TimeStamp باید با تاریخ جاری سیستم مقارنه می شود.

جزئیات فراخوانی این متد در جدول زیر شرح داده شده است.

https://pep.shaparak.ir/Api/v1/Payment/VerifyPayment		آدرس
POST		متد
توضیحات	نوع فیلد	نام فیلد(موارد ستاره دار ضروری می باشد)
فرمت محتوی درخواست Application/json	String	Content-Type *
امضای دیجیتال پارامترهای ورودی(پیوست ۲)	String	Sign *
شماره فاکتور	String	InvoiceNumber *
تاریخ فاکتور	String	InvoiceDate *
کد ترمینال	Int	TerminalCode *
کد پذیرنده	Int	MerchantCode *
مبلغ تراکنش	Decimal	Amount *
زمان ارسال تراکنش با فرمت 2018/09/18 15:15:13	String	TimeStamp *
False   True	Bool	IsSuccess
پیغام	String	Message
شماره کارت خریدار به صورت Mask شده	String	MaskedCardNumber
شماره کارت خریدار به صورت Hash شده	String	HashedCardNumber
شماره ارجاع شاپرکی	String	ShaparakRefNumber
	ورودی	خروجی
		موفق
		<pre>{   "IsSuccess": true,   "Message": "عملیات با موفقیت انجام شد",   "MaskedCardNumber": "5022-29**-****-2328",   "HashedCardNumber":     "2DDB1E270C598677AE328AA37C2970E3075E1DB6665C5AAFD13     1C59F7FAD99F23680536B07C140D24AAD8355EA9725A5493AC48     E0F48E39D50B54DB906958182",   "ShaparakRefNumber": "100200300400500" }</pre>
		ناموفق
		<pre>{   "IsSuccess": false,   "Message": "تراکنش ارسالی معتبر نیست" }</pre>
	کد پاسخ HTTP	موفق: 200 Ok

## ۷. برگشت از خرید

در صورتی که فروشنده به هر دلیلی مایل به برگشت زدن خرید باشد، می تواند حداکثر تا دو ساعت پس از انجام تراکنش خرید این کار را توسط فراخوانی متد Refund انجام دهد.

توجه شود که برای تراکنش های برگشت از خرید، پذیرنده باید شماره فاکتور و تاریخ فاکتور تراکنش خرید (تراکنش اصلی) را ارسال کند ولی Timestamp باید با تاریخ جاری سیستم مقاردهی شود. جزئیات فراخوانی این متد در جدول زیر شرح داده شده است.

https://pep.shaparak.ir/Api/v1/Payment/RefundPayment			آدرس
POST			متد
توضیحات	نوع فیلد	نام فیلد(موارد ستاره دار ضروری می باشد)	
فرمت محتوی درخواست Application/json	String	Content-Type *	
امضای دیجیتال پارامترهای ورودی(پیوست ۲)	String	Sign *	
شماره فاکتور	String	InvoiceNumber *	
تاریخ فاکتور	String	InvoiceDate *	
کد ترمینال	Int	TerminalCode *	
کد پذیرنده	Int	MerchantCode *	
زمان ارسال تراکنش با فرمت 2018/09/18 15:15:13	String	TimeStamp *	
False   True	Bool	IsSuccess	
پیغام	String	Message	
خروجی	ورودی		
موفق			
{ "IsSuccess": true, "Message": "عملیات با موفقیت انجام شد." }			
ناموفق			
{ "IsSuccess": false, "Message": "تراکنش ارسالی معتبر نیست." }			
موفق: 200 Ok			کد پاسخ HTTP

## ۸. استفاده از swagger جهت تست و فراخوانی سرویس ها

با استفاده از آدرس <https://pep.shapark.ir/swagger/ui/index> می توانید لیست کلیه سرویس های پرداخت ، به همراه توضیحات مربوطه ، فرمت پارامترهای ورودی و خروجی همچنین نمونه اطلاعات جهت فراخوانی وب سرویس ها را مشاهده نمایید. به طور مثال جهت آگاهی از نحوه فراخوانی متد VerifyPayment ، با مراجعه به آدرس مذکور می توان این مورد را از لیست سرویس ها پیدا کرده و ورودی و خروجی ها را مشاهده نمود.

POST /Api/Payment/VerifyPayment

در صورتی که عملیات خرید با موفقیت انجام شده باشد، درگاه پرداخت مدت زمان مشخصی منتظر می ماند تا خرید انجام شده توسط فروشنده تایید شود. در صورتی که خرید طی این مدت زمان توسط پذیرنده تایید نشود درگاه به صورت خودکار آن را برگشت زده و پول به حساب خریدار باز می گردد. مدت زمانی که بانک برای تایید خرید از سمت پذیرنده منتظر می ماند طبق توافق بانک و پذیرنده می باشد. در نتیجه پذیرنده پس از دریافت نتیجه تراکنش می بایست از طریق فراخوانی متد VerifyPayment در وبسرویس پرداخت الکترونیک پاسارگاد اقدام به تایید خرید خریدار خود نماید. توجه شود که برای تایید خرید، پذیرنده باید شماره فاکتور و تاریخ فاکتور تراکنش خرید (تراکنش اصلی) را ارسال کند ولی Timestamp باید با تاریخ جاری سیستم مقارن باشد.

Implementation Notes

Sample request:

```
{ "InvoiceNumber": "920", "InvoiceDate": "2019/01/27 17:57:06", "TerminalCode": "550363", "MerchantCode": "550166", "Amount": 10000, "Timestamp": "2019/01/27 17:57:06", }
```

Response Class (Status 200)

OK

Model Example Value

```
{ }
```

Response Content Type application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type
invoiceDetail	(required)	جزئیات درخواست	body	Model Example Value
	Parameter content type: application/json			<pre>{   "Amount": "string",   "InvoiceNumber": "string",   "InvoiceDate": "string",   "MerchantCode": "string",   "TerminalCode": "string",   "TimeStamp": "string",   "Sign": "string" }</pre>
Sign		امضاء	header	string

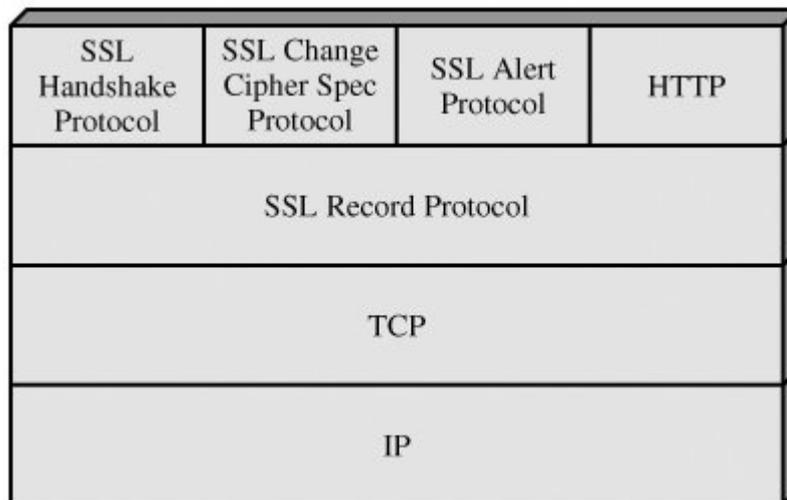
Try it out!

با وارد کردن پارامتر invoicedetail در باکس مربوطه همانند نمونه ورودی (sample request) و همین طور پارامتر امضا، و زدن دکمه Try it Out می توانید این سرویس را فراخوانی کرده و نتیجه آن را در همین قسمت مشاهده نمایید.

## پیوست ۱: نیازمندی های امنیتی

جهت برقراری ارتباط امن فیما بین سایت پذیرنده و سایت بانک، سایت بانک از پروتکل SSL استفاده می کند. پروتکل SSL (Secure Socket Layer) یک استاندارد وب برای رمزنگاری اطلاعات بین کاربر و وب سایت است. اطلاعاتی که توسط یک اتصال SSL مبادله می شوند بصورت رمز شده ارسال می شوند و بدین ترتیب اطلاعات مبادله شده از دزدیده شدن یا استراق سمع محافظت می شوند. SSL برای شرکت ها و مشتریان این امکان را فراهم می کند که بتوانند با اطمینان

اطلاعات خود (مانند شماره کارت اعتباری و ...) را به یک وب سایت بطور محرمانه ارسال کنند. برای برقراری یک اتصال SSL نیاز به یک SSL Certificate می باشد. همچنین پیشنهاد می شود که سایت پذیرنده نیز از پروتکل SSL استفاده کند اما اجباری نیست.



یکی دیگر از نیازمندی های امنیتی این است که پذیرنده نباید از هیچ کدام از اطلاعات مالی خریدار (همانند مشخصات کارت، کلمه رمز کارت و ...) مطلع شود. به همین دلیل پذیرنده از مشتری هیچ نوع اطلاعات مالی و بانکی دریافت نمی کند و تمامی این اطلاعات توسط خریدار صرفاً در درگاه پپ وارد می شود.

## پیوست ۲: نحوه ایجاد امضای دیجیتال

یکی دیگر از نیازمندی‌های امنیتی این است که پذیرنده می‌بایست تمامی بدنه درخواست که به فرمت json می‌باشد را امضا کرده و نتیجه‌ی حاصله را در یک هدر با عنوان Sign برای متد مورد نظر در وب‌سرویس ارسال نماید. با کمک این امضای دیجیتال درگاه پرداخت پپ از بابت صحت اطلاعات ارسالی از طرف پذیرنده، اطمینان حاصل می‌نماید. مثالی از نحوه‌ی ایجاد امضای دیجیتال به زبان C# در زیر آمده است.

```
public string GetSign(string data)
{
    var cs = new CspParameters { KeyContainerName = "PaymentTest" };
    var rsa = new RSACryptoServiceProvider(cs) { PersistKeyInCsp = false };

    rsa.Clear();
    rsa = new RSACryptoServiceProvider();
    rsa.FromXmlString("<RSAKeyValue><Modulus>2vW514pF6e2xBe4L0pq197o2/Xm6A4ktgYme+S/7SAQglFYb9swyrXzeeZGM0FDzi-UuxPJpCmG85As35L3PBHc5D/cVwt7HyrgoygXguzIVFLQPcS-kG1Phiu/9wXF1+wt579Jl0apjYIM99vzsw1X8W5HMMW002snNR4Gh+KujE=</Modulus><Exponent>AQAB</Exponent><P>7TpcqQxQSnxQuGxg1gAExDjkLZRu-WXMsMZ1HcGs9B659ZCtyx0K9PZeBb+rSbsDiQ53ME7gfr1qez5OJs8V3Kw==</P><Q>7E1MHADjw9SjcIoA9ZiEtdZN-lesfuxImTJ3ZSgVJLHm1DzpdDZizOipMcoJB30p9DUybV0yA92Ks9vPON1emEw==</Q><DP>M5IXaKyDm92wkpWbLgps/tc7S21UH9/4wIRnbInxt4TIP41ud0Db8NLJ0bGjs239AiQAp-FzHjpBNq+Rv8APCZw==</DP><DQ>t1v15PFHzorvPgDJ18xAh/9Ce+1W2UuvTtt-baFaLvYi/0Y74Qa56vs5S9DVius1KF4zwKyGiHteDE6yExWuN4w==</DQ><InverseQ>ps0bU-jxFx2RxXgvA8nU+C+RSGVI3UgoUMD9L+asg2YrCSj11S1RQqu4Yh+bkIY3sb58/5VpzRZ1/Dufdz1/LFw==</InverseQ><D>0hw2yioPTfsgHRPFHXqjyoAoMfNJU8DnS9arUzTRupY101hbCY+9718Ra-DAhr/Ob/pcrDaVfATEbamWjUt2kpXe6R5TQ7dfShxNqbBgQtPBXvjuho0tU6mFOWSyE-GQUEsVsVSexvJyM/I1aXj9m9BHVSpo6p6+Jb5yYM/G2PnbU=</D></RSAKeyValue>");

    byte[] signMain = rsa.SignData(Encoding.UTF8.GetBytes(data), new
    SHA1CryptoServiceProvider());
    string sign = Convert.ToBase64String(signMain);
    return sign;
}
```

### پیوست ۳: نمونه کد فراخوانی سرویس های درگاه پرداخت

نمونه کد فراخوانی سرویس دریافت مجوز پرداخت (Token) به زبان C# به شرح زیر می باشد. لازم به ذکر است جهت فراخوانی تمامی سرویس های درگاه پرداخت می توان از قطعه کد زیر استفاده نمود، به صورتی که تنها می بایست آدرس متد مورد نظر و مقدار json ورودی آن متد در کد زیر قرار گیرد.

```
public static string CallPaymentMethod()
{
    var sendingData = "{ \"InvoiceNumber\": \"123456\", \"InvoiceDate\": \"1349/04/04\", \"TerminalCode\": \"1\", \"MerchantCode\": \"1\", \"Amount\": \"1000\", \"RedirectAddress\": \"https://www.sample.com/PaymentResult\", \"Timestamp\": \"2018/09/18 15:15:13\", \"Action\": \"1003\", \"Mobile\": \"0912222222\", \"Email\": \"BuyerName@Sample.ir\" }";

    var content = new StringContent(sendingData, Encoding.UTF8, "application/json");
    var request = new HttpRequestMessage
    {
        RequestUri = new Uri("https://pep.shaparak.ir/Api/v1/Payment/GetToken"),
        Method = HttpMethod.Post,
        Content = content
    };

    request.Headers.Add("Sign", GetSign(sendingData));

    var client = new HttpClient();
    client.DefaultRequestHeaders.Accept.Add(new
        MediaTypeWithQualityHeaderValue("application/json"));

    var response = client.SendAsync(requestMessage).Result;
    return Encoding.UTF8.GetString(response.Content.ReadAsByteArrayAsync().Result);
}
```

## پیوست ۴: نمونه کد HTML هدایت مشتری به درگاه پرداخت

سایت پذیرنده پس از دریافت توکن پرداخت از طریق متد GetToken اقدام به نمایش فرم زیر به مشتری خود می‌نماید. مشتری با کلیک بر روی گزینه "ارسال به درگاه" به درگاه پرداخت بانک منتقل شده و عملیات پرداخت خود را تکمیل می‌نماید.

```
<form id="PaymentForm" method="post" Action="https://pep.shaparak.ir/payment.aspx" >  
<input type="hidden" name="Token" value="توکن دریافتی از طریق وب سرویس" />  
<input type="submit" name="submit" value="ارسال به درگاه" />  
</form>
```

## پیوست ۵: الگوریتم رمز نگاری نامتقارن

الگوریتم‌های رمز گذاری نامتقارن نوعی از الگوریتم‌های رمز نگاری هستند که دارای دو کلید مختلف می‌باشند که از یکی جهت رمزنگاری و از دیگری جهت رمز گشایی استفاده می‌شود. این الگوریتم‌ها در گستره وسیعی از کاربردها به کار می‌رود. در این الگوریتم‌ها کلید اول را کلید عمومی (Public Key) و کلید دوم را کلید خصوصی (Private Key) می‌نامند. یکی از کاربردهای مهم الگوریتم‌های رمز نگاری نامتقارن استفاده از آنها در تولید امضای دیجیتال می‌باشد.

### مفهوم امضای دیجیتال

امضای دیجیتال روشی مبتنی بر الگوریتم‌های رمزنگاری نامتقارن می‌باشد که به کمک آن می‌توان اطمینان حاصل کرد که داده‌های ارسالی از جانب شخص مشخصی ارسال شده است. نمونه ای از این الگوریتم‌ها می‌توان به RSA و DSA اشاره کرد.

روال کار در امضای دیجیتال به این شکل است که پیش از ارسال داده‌ها، اطلاعات را با استفاده از الگوریتم‌های درهم سازی یک‌طرفه (Hash Algorithms) به یک کد درهم (Hash) تبدیل می‌شود. از نمونه این الگوریتم‌ها می‌توان به MD5, SHA1 و ... اشاره کرد. یک‌طرفه بودن در این الگوریتم‌ها به این معنی است که پس از کد شدن اطلاعات به هیچ عنوان نمی‌توان از روی این کدها، اطلاعات اصلی را به دست آورد. پس از در هم سازی اطلاعات، به منظور تولید امضای دیجیتال، باید از یکی از الگوریتم‌های رمز نگاری نامتقارن استفاده شود، و با استفاده از کلید خصوصی (Private Key) آن الگوریتم، رشته‌ی تولید شده توسط الگوریتم درهم سازی را امضا نمود.

### مفهوم کلید عمومی و کلید خصوصی

کلید عمومی بخشی از کلید است که بین همه توزیع می‌شود و هیچ نگرانی از لو رفتن و دزدیده شدن آن وجود ندارد به واقع لفظ "عمومی" نیز بیان گر همین مطلب است. اگر داده‌ای برای صاحب کلید عمومی (پخش کننده کلید عمومی) باید رمز شود با استفاده از این کلید رمز نگاری شده و ارسال می‌شود. نکته مهم الگوریتم‌های نامتقارن در این مطلب است که داده‌های رمز شده با کلید عمومی فقط و فقط با کلید خصوصی قابل رمز گشایی هستند و دوباره با همان کلید عمومی نمی‌توان آنها را رمز گشایی کرد به همین دلیل داشتن کلید عمومی کمکی به رمز گشایی داده‌ها نخواهد کرد. کلید خصوصی در واقع بخشی از کلید است که به وسیله آن داده‌های رمز شده به وسیله کلید عمومی را می‌توان رمز گشایی کرد. صاحب کلید خصوصی باید حداکثر محافظت از این کلید را انجام دهد و به هیچ عنوان اجازه ندهد که این کلید در دست کسی غیر از خودش قرار گیرد. علاوه بر این با استفاده از کلید خصوصی می‌توان اسناد و مدارک مانند Document، Emailها و پیغامها را امضا کرد و امضای صورت گرفته را در انتهای Document، Email و یا پیغام قرار داد. در این حالت گیرنده پیغام با داشتن اصل پیغام، امضای دیجیتال زیر آن و کلید عمومی شما می‌تواند از صحت امضا اطمینان حاصل کند و مطمئن شود که داده‌ها از جانب شما ارسال شده است. اما با کلید عمومی به هیچ عنوان نمی‌تواند امضای شما را جعل کند.