

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

مستندات فنی



پرداخت الکترونیک
پاسارگاد

واحد پایانه های اینترنتی

فهرست مطالب

۳	۱. تعاریف.....
۳	۱-۱ تعاریف مرتبط با خریدار.....
۴	۲-۱ تعاریف مرتبط با پذیرنده.....
۸	۳-۱ تعاریف مرتبط با درگاه پرداخت و عملیات مالی.....
۹	۲. مراحل کلی فرآیند خرید.....
۱۰	۳. دریافت توکن پرداخت.....
۱۲	۴. ارجاع خریدار به درگاه پرداخت پپ.....
۱۲	۴-۱ ارسال خریدار به درگاه با استفاده از متد Get.....
۱۲	۴-۲ ارسال خریدار به درگاه با استفاده از متد Post.....
۱۳	۵. استعلام نتیجه تراکنش.....
۱۳	۵-۱ در صورت دریافت نتیجه تراکنش.....
۱۳	۵-۲ در صورت عدم دریافت نتیجه تراکنش.....
۱۶	۶. تایید خرید.....
۱۸	۷. برگشت از خرید.....
۱۹	۸. نحوه به روز رسانی یک دستور پرداخت.....
۲۱	۹. استعلام ریزپرداخت های ارسالی بر اساس تاریخ ریزپرداخت ها.....
۲۴	۱۰. استفاده از swagger جهت تست و فراخوانی سرویس ها.....
۲۵	پیوست ۱: نیازمندی های امنیتی.....
۲۶	پیوست ۲: نحوه ایجاد امضای دیجیتال.....
۲۷	پیوست ۳: نمونه کد فراخوانی سرویس های درگاه پرداخت.....
۲۸	پیوست ۴: نمونه کد HTML هدایت مشتری به درگاه پرداخت.....

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 تسهیم مبلغ پرداختی و واریز به حساب‌های جداگانه‌ی اعلامی توسط 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 وب سرویس 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 می‌تواند با ارسال یک دستور پرداخت هنگام خرید، مبالغی را در تاریخ‌های مشخص و به شماره حساب‌های مشخص واریز نماید. به عنوان مثال آژانس مسافرتی را در نظر بگیرید که می‌خواهد پس از پرداخت وجه از طریق درگاه پرداخت شرکت

پرداخت الکترونیک پاسارگاد توسط مشتری، قسمتی از این مبلغ به حساب هتل، قسمتی از آن به حساب آژانس هواپیمایی و .. در تاریخ‌های مشخص واریز گردد.

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 بانک به پذیرنده اختصاص می‌یابد و در حین انجام تراکنش برای شناسایی پذیرنده از آن استفاده می‌گردد.
- **شماره شناسائی ترمینال (TerminalCode):** کدی است که توسط بانک 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 بانک را با آن کلید، امضای دیجیتال می‌کند.
- **کلید عمومی پذیرنده (PublicKey):** کلیدی است که بانک جهت تایید امضای دیجیتال فروشگاه از آن استفاده می‌کند.
- **سپرده فروشنده:** شماره شبای پذیرنده می‌باشد که جهت انجام عمل تسویه حساب به شرکت پرداخت الکترونیک پاسارگاد اعلام می‌شود.
- **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 الگوریتم‌های رمزنگاری نامتقارن می‌باشد که به کمک آن می‌توان اطمینان حاصل کرد که داده‌های ارسالی از جانب فروشگاه مشخصی ارسال شده است.

- **آدرس بازگشت (RedirectAddress):** آدرس صفحه‌ای در سایت پذیرنده است که خریدار پس از انجام عملیات خرید به آن فرستاده می‌شود.
- **Timestamp:** زمان ارسال داده به درگاه پرداخت را Timestamp می‌گویند که فرمت آن به شکل "YYYY/MM/DD HH:MM:SS" بوده و به تاریخ میلادی ارسال می‌گردد. اگر هر کدام از عده‌های 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. نکته‌ی مهم در اینجا این است که مقداری که در فیلد Timestamp قرار می‌گیرد باید دقیقاً با مقداری که تحت همین عنوان در امضای دیجیتال قرار می‌گیرد یکی باشد، همچنین هیچ دو درخواستی، نمی‌توانند دارای Timestamp یکسان باشند.
- **تلفن همراه (Mobile):** شماره تلفن همراه خریدار است که توسط فروشگاه برای درگاه پرداخت ارسال می‌گردد. در صورت ارسال این فیلد توسط فروشگاه، درگاه پرداخت، شماره کارت‌های ثبت شده کاربر در سامانه پیوند را نمایش می‌دهد و در غیراینصورت هیچ شماره کارت‌ی نمایش داده نمی‌شود. همچنین در صورت ارسال این فیلد، کاربر می‌تواند 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" می‌باشد.
- **پست الکترونیک (Email):** آدرس پست الکترونیک خریدار است که می‌تواند توسط وب سایت فروشگاه به درگاه پرداخت ارسال شود. در صورت ارسال این فیلد توسط فروشگاه، فیلد ایمیل در درگاه پرداخت با آدرس آرسالی پر می‌شود.
- **نام پذیرنده (MerchantName):** نام پذیرنده است که می‌تواند توسط وب سایت فروشگاه به درگاه پرداخت ارسال شود. در صورت ارسال این فیلد توسط فروشگاه، فیلد نام فروشگاه در درگاه پرداخت با نام آرسالی پر می‌شود، 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.
- **شناسه پرداخت (PIDN):** شناسه خرید مورد نظر پذیرنده است که در صورت نیاز می‌بایست با فرمت عنوان شده در پیوست ۵ به درگاه پرداخت اینترنتی ارسال شود.

- لیست ریزپرداختها (SubPaymentList): یک xml از لیست ریزپرداختها به صورت زیر می باشد که به رشته ای با فرمت base64String تبدیل می شود.

```
<?xml version="1.0" encoding="utf-8"?>
<SubPaymentList>
  <SubPayments>
    <SubPayment>
      <SubPayID>1</SubPayID>
      <Amount>5000000</Amount>
      <Date>2010/02/02</Date>
      <Account>219.10.44039.1</Account>
      <Description></Description>
    </SubPayment>
    <SubPayment>
      <SubPayID>2</SubPayID>
      <Amount>30000</Amount>
      <Date>2010/04/08</Date>
      <Account>201.800.981313.1</Account>
      <Description></Description>
    </SubPayment>
    .
    .
  </SubPayments>
</SubPaymentList>
```

SubPayID: شناسه ریزپرداخت می باشد.

Amount: مبلغ ریزپرداخت می باشد.

Date: تاریخ واریز وجه می باشد.

Account: شماره شبا یا شماره حساب جهت واریز وجه می باشد.

Description: توضیحات تکمیلی می باشد.

- لیست به روزرسانی ریزپرداختها (InvoiceUpdateList): یک xml از لیست ریزپرداختهای نیازمند به روزرسانی به فرمت زیر می باشد. لازم به ذکر است که این XML بعد از تشکیل می بایست به فرمت base64String تبدیل شود.

```
<?xml version="1.0" encoding="utf-8"?>
<invoiceUpdateList>
  <invoiceAction invoiceUID="634253256472082172">
    <action type="Add" subPayID="4" amount="1" date="2010/02/02" account="219.10.44039.1"/>
    <action type="Delete" subPayID="5" amount="2" date="2010/02/02" account="219.10.44039.1"/>
    <action type="Edit" subPayID="1" amount="1" date="2010/02/02" account="219.10.44039.1"/>
    <action type="Add" subPayID="2" amount="1" date="2010/02/02" account="219.10.44039.1"/>
  </invoiceAction>
</invoiceUpdateList>
```

نکته ۱: نوع انتقال در زمان ویرایش یک رکورد باید با نوع قبلی آن یکی باشد. به طور مثال چنانچه نوع انتقال ریزپرداخت واریز به حساب است نمی توان نوع آن را به انتقال به شبا تغییر داد.

نکته ۲: لازم به ذکر است که تا زمانی می توان هر یک از عملیات Delete و Edit را بر روی یک ریزپرداخت انجام داد که آن ریزپرداخت در حالت فعال باشد، یعنی هنوز زمان انجام آن فرا نرسیده و یا به هر دلیل انجام نشده باشد. همچنین عملیات Add

واحد پایانه های اینترنتی شرکت پرداخت الکترونیک پاسارگاد

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

صفحه ۷

PEP IPG REST MultiPayment.13971124.Ver3.00

۱۳۹۷/۱۱/۲۴



(اضافه کردن یک ریزپرداخت) را در صورتی می توان انجام داد که مجموع مبالغ ریزپرداخت ها پس از به روزرسانی بیشتر از مبلغ پرداخت شده برای فاکتور نباشد. در این صورت به روزرسانی انجام نشده و ریزپرداخت ها در همان حالت قبلی خود باقی می ماند.

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 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 اعلامی توسط 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		
https://pep.shaparak.ir/Api/v1/Payment/GetToken		
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
SelectedLanguage	String	En Fa
PIDN	String	شناسه پرداخت (پیوست ۵)
SubPaymentList *	String	جزئیات ریزپرداخت‌ها با فرمت base64String
IsSuccess	Boolean	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 IPG



شرکت پرداخت الکترونیک
پاسارگاد

صفحه ۱۱

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 می بایست خریدار را همراه با توکن دریافتی به درگاه پرداخت هدایت کند. پذیرنده می تواند 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 می تواند 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 می بایست 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 می بایست توکن دریافتی را با متد HTTP POST به سایت پپ <https://pep.shaparak.ir/payment.aspx> ارسال نماید. فرم ارسالی از سایت پذیرنده می بایست 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 می نماید. در این مرحله تراکنش توسط درگاه پپ پردازش گردیده و عملیات لازم در مرکز شاپرک و بانک صادرکننده کارت انجام می پذیرد.

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

- 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 IPG



صفحه ۱۴

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	Boolean	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		

<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 IPG



صفحه ۱۷

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 باشند)
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	Boolean	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
خروجی		ورودی
موفق		
<pre>{ "IsSuccess": true, "Message": "عملیات با موفقیت انجام شد", "MaskedCardNumber": "5022-29**-*2328", "HashedCardNumber": "2DDB1E270C598677AE328AA37C2970E3075E1DB6665C5AAFD13 1C59F7FAD99F23680536B07C140D24AAD8355EA9725A5493AC48 EOF48E39D50B54DB906958182", "ShaparakRefNumber": "100200300400500" }</pre>		
ناموفق		
<pre>{ "IsSuccess": false, "Message": "تراکنش ارسالی معتبر نیست" }</pre>		
موفق: 200 Ok		کد پاسخ HTTP

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 باشند)	
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	Boolean	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. نحوه به روز رسانی یک دستور پرداخت

فروشنده در دو حالت می تواند ریزپرداخت های فاکتور ارسالی را به روز کند:

- در حالتی که پذیرنده اقدام به دریافت توکن نموده باشد و به هر دلیلی خریدار اقدام به پرداخت وجه در پپ نموده باشد، پذیرنده این امکان را دارد که با دریافت مجدد توکن اقدام به بروزسانی فاکتور مربوطه و تغییر ریزپرداخت های آن نماید. جهت بروزسانی فاکتور از پیش ثبت شده، پذیرنده می بایست اطلاعات همان فاکتور (شماره، تاریخ و مبلغ) را به همراه لیست ریزپرداخت های جدید ارسال نمایند. در ضمن مقدار TimeStamp ارسالی نیز باید تغییر یافته باشد. بدین ترتیب لیست جدید جایگزین لیست قبلی شده و در تاریخ های مشخص شده پرداخت صورت می گیرد.

۲. پس از تایید خرید، برای به روزرسانی ریزپرداخت‌های این فاکتور سایت پذیرنده می‌بایست اطلاعات مربوط به فاکتور ویرایش شده را با PrivateKey خود امضا کرده و از طریق متد UpdateInvoiceSubPayment برای سیستم پپ ارسال نماید. لازم به ذکر است مجموع مبلغ ریزپرداخت‌ها می‌بایست برابر یا کمتر از مبلغ فاکتور باشد. جزئیات فراخوانی این متد در جدول زیر شرح داده شده است.

https://pep.shaparak.ir/Api/v1/Payment/UpdateInvoiceSubPayment			آدرس
POST			متد
توضیحات	نوع فیلد	نام فیلد (موارد ستاره دار ضروری می‌باشند)	
فرمت محتوی درخواست Application/json	String	Content-Type *	
امضای دیجیتال پارامترهای ورودی (پیوست ۲)	String	Sign *	
لیست به روزرسانی ریزپرداخت‌ها (بخش ۱-۲)	String	InvoiceUpdateList *	
کد ترمینال	Int	TerminalCode *	
کد پذیرنده	Int	MerchantCode *	
زمان ارسال تراکنش با فرمت 2018/09/18 15:15:13	String	TimeStamp *	
False True	Boolean	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

۹. استعلام ریزپرداخت‌های ارسالی بر اساس تاریخ ریزپرداخت‌ها

پذیرنده می‌تواند اطلاعات مربوط به استعلام ریزپرداخت‌ها را با PrivateKey خود امضا کرده و از طریق فراخوانی متد GetSubPaymentsReport از وضعیت کنونی این ریزپرداخت‌ها اطلاع حاصل نماید. جزئیات فراخوانی این متد در جدول زیر شرح داده شده است.

نام فیلد(موارد ستاره‌دار ضروری می‌باشند)	نوع فیلد	توضیحات
آدرس	https://pep.shaparak.ir/Api/v1/Payment/GetSubPaymentsReport	
متد	POST	
Content-Type *	String	فرمت محتوی درخواست Application/json
Sign *	String	امضای دیجیتال پارامترهای ورودی (پیوست ۲)
MerchantCode *	Int	کد پذیرنده
TerminalCode *	Int	کد ترمینال
StartDate *	String	ابتدای بازه‌ی گزارش
EndDate *	String	انتهای بازه‌ی گزارش
TimeStamp *	String	زمان ارسال تراکنش با فرمت 2018/09/18 15:15:13
IsSuccess	Boolean	False True
Message	String	پیغام
SubPayments	SubPayment[]	آرایه‌ای از ریزپرداخت‌ها
InvoiceUID	long	کد رهگیری فاکتور
SubPayID	Int	شناسه ریزپرداخت
Amount	Decimal	مبلغ ریزپرداخت
Date	DateTime	تاریخ ریزپرداخت
Account	String	شماره حساب یا شبا
Description	String	توضیحات
Status	String	Canceled Inactive Active Done
DepositName	String	نام سپرده
TransactionDate	DateTime	تاریخ تراکنش
PayaRefNumber	String	شماره پیگیری پایا
PayaStatus	String	آخرین وضعیت پایا (Unknown Confirmed Sent CentralBank_Rejected Sent_Recieved Rejected)
PayaStatusDesc	String	شرح آخرین وضعیت پایا
BankName	String	نام بانک مقصد در انتقال پایا

واحد پایانه های اینترنتی شرکت پرداخت الکترونیک پاسارگاد



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

صفحه ۲۲

PEP IPG REST MultiPayment.13971124.Ver3.00

۱۳۹۷/۱۱/۲۴

خروجی	ورودی	نمونه Json
موفق		
<pre>{ "IsSuccess": true, "Message": "عملیات با موفقیت انجام شد", "SubPayments": [{ "InvoiceUID": 636872081134425100, "SubPayID": 1, "Amount": "50000", "Account": "IR680570031980010098922001", "Date": "03/04/2019 12:00:00 ق.ظ", "Description": "", "Status": "Inactive", "DepositName": null, "TransactionDate": null, "PayaRefNumber": null, "PayaStatus": "unknown", "PayaStatusDesc": "نامشخص", "BankName": "پاسارگاد" }] }</pre>		
ناموفق		
<pre>{ "IsSuccess": false, "Message": "تراکنش ارسالی معتبر نیست" }</pre>		
موفق: 200 Ok		کد پاسخ HTTP

نکته ۱: چهار فیلد PayaRefNumber، PayaStatusDesc، PayaStatus، BankName در خروجی چنانچه ریزپرداختی به صورت پایا انجام شود معتبر می باشند.

نکته ۲: فیلد PayaStatusDesc شامل مقادیر زیر است که در واقع عنوان فارسی متناظر با PayaStatus است:

- نامشخص (Unknown): وضعیت انتقال نامشخص است.
- ارسالی - تایید شده (Confirmed): درخواست انتقال با موفقیت ثبت شده است.
- ارسالی - ارسال شده به بانک مرکزی (Sent): درخواست انتقال به بانک مرکزی ارسال شده است.
- ارسالی - رد شده توسط بانک مرکزی (CentralBank_Rejected): درخواست انتقال ارسالی، توسط بانک مرکزی مردود شده است.

واحد پایانه های اینترنتی شرکت پرداخت الکترونیک پاسارگاد



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

صفحه ۲۳

PEP IPG REST MultiPayment.13971124.Ver3.00

۱۳۹۷/۱۱/۲۴

- ارسالی - دریافت شده توسط بانک مرکزی (Sent_Recieved): درخواست انتقال توسط بانک مرکزی دریافت شده است.
- ارسالی - رد شده توسط بانک مقابل (Rejected): بانک مقصد درخواست انتقال را به هر دلیل رد کرده است.

نکته ۳: فیلد Status می تواند شامل حالت های زیر باشد:

- **Inactive:** به این معناست که فاکتور ارسالی پرداخت نشده است و ریز پرداخت مورد نظر در حالت غیرفعال است. به محض پرداخت مبلغ فاکتور ریزپرداخت مورد نظر فعال می شود.
توجه: در خرید دو مرحله ای ریزپرداخت ها پس از تایید خرید توسط فروشگاه فعال می شوند.
- **Active:** به این معناست که فاکتور ارسالی پرداخت شده است و ریزپرداخت مورد نظر آماده است تا در تاریخ مشخص شده انجام شود، و یا به هر دلیلی ریز پرداخت در تاریخ مورد نظر پرداخت نشده و مجدداً برای پرداخت آن تلاش می شود.
- توجه: تا زمانی که ریزپرداخت در حالت فعال باشد و به هر دلیلی (به عنوان مثال کافی نبودن موجودی حساب فروشگاه) با موفقیت انجام نشود، هر روز برای انجام آن تلاش خواهد شد مگر اینکه که فروشگاه آن را لغو کند.
- **Done:** بدین معناست که ریزپرداخت با موفقیت پرداخت شده است.
- **Canceled:** بدین معناست که ریزپرداخت توسط فروشگاه لغو شده است.
- توجه: در صورتی که فروشگاه از خرید دو مرحله ای استفاده می کند در صورت تایید نکردن خرید، خرید برگشت خورده و ریزپرداخت های آن نیز لغو می شوند.

۱۰. 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 وب سرویس 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 مقاردهی شود

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

Parameters

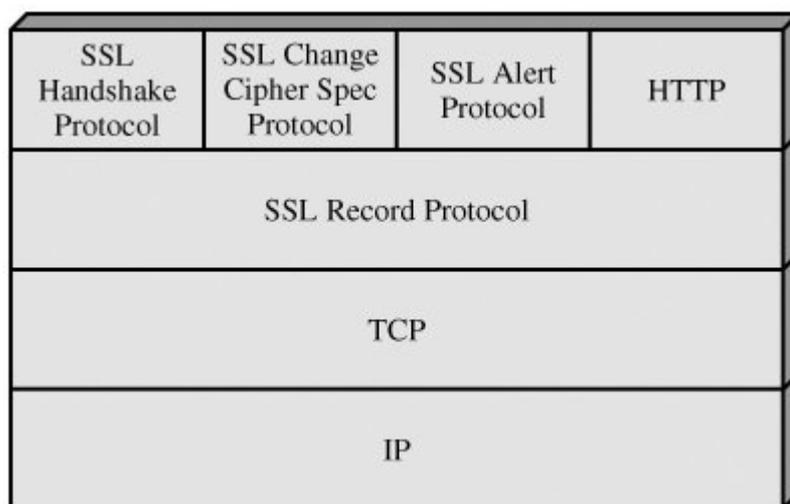
Parameter	Value	Description	Parameter Type	Data Type
invoiceDetail	(required)	جزئیات درخواست	body	Model Example Value
	Parameter content type: <input type="text" value="application/json"/>			<pre>{ "Amount": "string", "InvoiceNumber": "string", "InvoiceDate": "string", "MerchantCode": "string", "TerminalCode":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

با وارد کردن پارامتر invoiceDetail در باکس مربوطه همانند نمونه ورودی (sample request) و همین طور پارامتر امضاء، و زدن دکمه Try it Out می توانید این سرویس را فراخوانی کرده و نتیجه آن را در همین قسمت ملاحظه 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+wt579JloapjYIM99vzsw1X8W5HMMW002snNR4Gh+KujE=</Modulus><Exponent>AQAB</Exponent><P>7TpcqQxQSnxQuGXg1gAExDjkLZRu-WXMsMZ1HcGs9B659ZCtyx0K9PZeBb+rSbsDiQ53ME7gfr1qez5OJs8V3Kw==</P><Q>7E1MHADjw9SjcIoA9ZiEtdZN-lesfuxImTJ3ZSgVJLHm1DzpdDZiz0iPMcoJB30p9DUybV0yA92Ks9vPON1emEw==</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/I1aXj9m9BHVS0gp6+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 می نماید. مشتری با کلیک بر روی گزینه "ارسال به درگاه" به درگاه پرداخت بانک منتقل شده و عملیات پرداخت خود را تکمیل می نماید.

```
<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 اعتبار سنجی شناسه پرداخت

شناسه پرداختی که به سمت درگاه پرداخت اینترنتی ارسال می شود باید از ساختار زیر تبعیت کند تا معتبر شناخته شود، در غیر این صورت پذیرنده با پیغام خطا مواجه می شود.

- شماره شناسه: رقم کنترلی (۲ کاراکتر) + شماره سریال (بین ۳ تا ۱۷ کاراکتر) "-" شماره حساب (حداکثر ۱۰ کاراکتر)
- شماره حساب: شماره سپرده مشتری بدون نقطه
- شماره سریال: ترکیب پارامترهای تعریف شده توسط کاربر به صورت رشته ای
- رقم کنترلی: محاسبه شده بر اساس شماره حساب، سریال و مبلغ
نکته: مبلغ می بایست کمتر از ۱۵ رقم باشد.

نحوه محاسبه رقم کنترلی:

الف: کلیه کاراکترهای سریال از سمت راست در اعداد اول به شرح زیر ضرب شده و حاصل جمع آنها برابر مقدار پارامتر A خواهد بود

بود															
موقعیت مکانی از سمت راست	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
اعداد اول	۵۳	۴۷	۴۳	۴۱	۳۷	۳۱	۲۹	۲۳	۱۹	۱۷	۱۳	۱۱	۷	۵	۳

ب: اعداد شماره حساب از سمت راست در اعداد اول به شرح زیر ضرب شده و حاصل جمع آنها برابر مقدار پارامتر B خواهد بود

ضرب													
موقعیت مکانی از سمت راست	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰			
اعداد اول	۳۷	۳۱	۲۹	۲۳	۱۹	۱۷	۱۳	۱۱	۷	۵			

ج: مبلغ از سمت راست در اعداد اول به شرح زیر ضرب شده و حاصل جمع آنها برابر مقدار پارامتر C خواهد بود

ضرب															
موقعیت مکانی از سمت راست	۱	۲	۳	۴	۵	۶	۷	۸	۹	۱۰	۱۱	۱۲	۱۳	۱۴	۱۵
اعداد اول	۶۱	۵۹	۵۳	۴۷	۴۳	۴۱	۳۷	۳۱	۲۹	۲۳	۱۹	۱۷	۱۳	۱۱	۷

د: $[(A+B+C) \text{Mod } 99]$

واحد پایانه های اینترنتی شرکت پرداخت الکترونیک پاسارگاد

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



صفحه ۳۰

PEP IPG REST MultiPayment.13971124.Ver3.00

۱۳۹۷/۱۱/۲۴

مثال:

شناسه: ۱۸۰۰۰۷۶۲۱-۱۲۳۴۲۵

سریال: ۱۲۳۴

شماره حساب: ۱۸۰۰۰۷۶۲۱

مبلغ: ۱۲۵۰۰

رقم کنترلی: ۲۵

الف:

۱	۲	۳	۴	شناسه
۴۱	۴۳	۴۷	۵۳	اعداد اول
۴۱	۸۶	۱۴۱	۲۱۲	حاصلضرب
			۴۸۰	حاصلجمع

ب:

۱	۸	۰	۰	۰	۷	۶	۲	۱	شماره حساب
۷	۱۱	۱۳	۱۷	۱۹	۲۳	۲۹	۳۱	۳۷	اعداد اول
۷	۸۸	۰	۰	۰	۱۶۱	۱۷۴	۶۲	۳۷	حاصلضرب
								۵۲۲	حاصلجمع

ج:

۱	۲	۵	۰	۰	مبلغ
۴۳	۴۷	۵۳	۵۹	۶۱	اعداد اول
۴۳	۹۴	۲۶۵	۰	۰	حاصلضرب
				۴۰۲	حاصلجمع

$$د: ۲۵ = [(۴۸۰ + ۵۲۲ + ۴۰۲) \text{Mod } ۹۹]$$

پیوست ۶: 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.