

راه‌نمای اتصال به

درگاه پرداخت امن پاسارگاد

نمایه

۳.....	رویه‌ی انجام تراکنش با درگاه پرداخت امن پاسارگاد
۳.....	محتوای sign
۳.....	محتوای content
۶.....	دریافت نتیجه تراکنش

رویه‌ی انجام تراکنش با درگاه پرداخت امن پاسارگاد

خریدار با مراجعه به سایت فروشگاه، کالا یا کالاهای مورد نظر خود را انتخاب کرده و توسط سایت فروشگاه به درگاه پرداخت امن ارجاع داده می‌شود. این ارجاع با متود POST و به آدرس <https://paypaad.bankpasargad.com/PaymentController> از سیستم پرداخت امن خواهد بود. پارامترهای ارسالی به این آدرس content و sign هستند که به ترتیب اطلاعات فاکتور مشتری و امضای دیجیتال تولید شده توسط فروشگاه هستند. توجه شود که درخواست https باشد.

محتوای sign

از آنجا که درگاه پرداخت امن با تراکنش‌های مالی سر و کار دارد، وجود مکانیزم‌های کارا برای تضمین امنیت تراکنش‌های ارسالی به درگاه اجتناب ناپذیر است. این خواسته مهم با استفاده از مفهوم امضای دیجیتال تامین شده است.

پارامتر sign در درخواست ارسالی به درگاه امن، حاوی امضای دیجیتال داده‌ی موجود در پارامتر content است تا به این ترتیب بتوان از صحت اعتبار فرستنده‌ی درخواست تراکنش اطمینان حاصل کرد. در مرحله ثبت فروشگاه در درگاه امن، به هر فروشگاه یک کلید خصوصی¹ یکتا اختصاص داده می‌شود که فروشگاه باید این کلید را به صورت محرمانه نگهداری کنند و از انتشار آن پرهیز کنند، چه آن‌که اگر این کلید به دست شخص دیگری بیفتد، آن شخص توانایی آن‌را دارد که از جانب آن فروشگاه درخواست ارسال کند. کلید مختص فروشگاه است و حتی در درگاه پرداخت امن هم وجود ندارد، بلکه معادل کلید خصوصی، یک کلید عمومی وجود دارد که نزد درگاه پرداخت امن است و درگاه با استفاده از آن می‌تواند صحت امضای تولید شده را مورد ارزیابی قرار دهد. دقت شود که کلید عمومی همان کلید خصوصی نیست، بلکه یک جز کوچک از کلید خصوصی است و نمی‌توان با آن امضای دیجیتال تولید کرد، بلکه تنها می‌توان یک امضای تولید شده را ارزیابی نمود.

روال فرستادن یک درخواست به این طریق است که فروشگاه با استفاده از کلید خصوصی خود، امضای دیجیتال داده‌ای را که در پارامتر content ارسال می‌شود تولید کرده، آن‌را base64 می‌کند، حاصل را در پارامتر sign قرار می‌دهد و آن‌گاه درخواست خود را به درگاه پرداخت امن ارسال می‌نماید. لازم به ذکر است در مرحله‌ی تولید امضا داده به صورت SHA1 در هم سازی می‌شود و چون این روش برگشت ناپذیر است، از روی امضای تولید شده نمی‌توان داده را بازیابی کرد. برای شروع پیاده‌سازی نحوه‌ی تولید امضای دیجیتال در زبان‌های مختلف برنامه‌سازی، به نمونه کدهای ضمیمه‌ی این مستند مراجعه کنید.

محتوای content

یکی از پارامترهای ارسالی به درگاه پرداخت امن content است که حاوی XML ای با قالب مشخص است که در برگرفته‌ی اطلاعات فاکتور ارسالی از فروشگاه می‌باشد. شکل الف نمونه‌ی یک فاکتور فرضی در قالب XML است. فرمت XML ارسالی در فایل ضمیمه‌ی protocol.dtd موجود است.

¹ Private key

```

<invoice
time_stamp="2010/08/16 09:17:45"
timeout = "2011/09/05 09:17:45"
invoice_date="1389/12/13"
invoice_number="50788"
terminal_code="123456"
merchant_code="597100971"
redirect_address="http://localhost:8080/oradoSuccessPurchase.html?error=0"
referer_address="http://localhost:8080/oradoSuccessPurchase.html?error=1"
delivery_address="ده پلاك گلستان، خ نوبنياد، تهران،"
buyer_name="حسينى حسن"
buyer_tel="02122336655"
delivery_days="5">

<item number="2" event_date="2011/05/05 09:17:45" event_id="23659">
<content>تلويزيون</content>
<count>2</count>
<fee>10000</fee>
<description>كالا با مرتبط توضيحات</description>
<clearing>
<deposit code="1">20</deposit>
<deposit code="2">30</deposit>
</clearing>
</item>

<item number="1" event_date="2011/05/07 09:17:45" event_id="1122">
<content>ر اديو</content>
<count>30</count>
<fee>200</fee>
<amount>500</amount> <!-- just for backward compatibility -->
<description>كالا با مرتبط توضيحات</description>
<clearing>
<deposit code="1">40</deposit>
</clearing>
</item>

<item number="3" event_date="2011/05/06 09:17:45" event_id="8899">
<content>پلير دى وى دى</content>
<count>1</count>
<amount>1</amount> <!-- just for backward compatibility -->
<fee>10</fee>
<item_discount>2</item_discount>
<description>كالا با مرتبط توضيحات</description>
</item>

<item number="4">
<content>تخفيف</content>
<fee>-20</fee>
<count>1</count>
<description>تخفيف</description>
</item>

<item number="5">
<content>هما بليط</content>
<fee>60000</fee>
<count>1</count>
<cancel from="-10">
<percent>20</percent>
<constant>0</constant>
</cancel>
<description>كالا با مرتبط توضيحات</description>
</item>

<item number="6">
<content>قطار بليط</content>
<fee>1500</fee>
<count>1</count>
<cancel from="2011/04/08 09:17:45">
<percent>30</percent>
<constant>200</constant>
</cancel>
<description>كالا با مرتبط توضيحات</description>
</item>

<others>
<discount amount="5" description="ويژه تخفيف" />
<extra_cost amount="17" description="بستى هزينه" />
<discount amount="16" description="خاص مشتريان تخفيف" />
</others>
</invoice>

```

شکل الف، XML فرستاده شده در پارامتر content، حاوی اطلاعات فاکتور ارسالی به درگاه پرداخت

در مورد فاکتور باید به نکات زیر توجه شود:

- لازم است در XML ارسالی، کاراکترهای وابسته به سیستم عامل از قبیل \r، \n، \r\n و ... موجود نباشد.
- وجود این کاراکترها ممکن است باعث شود که sign ارسالی به درگاه تایید نشود و عملیات خرید لغو شود.
- هر فاکتور ارسالی شامل یک المان `<invoice />` است که مشخص کننده پارامترهای آن می باشد. این المان شامل فیلدهای مشخص، به شرح زیر است:
 - time_stamp: تاریخ ارسال درخواست به درگاه با فرمت "YYYY/MM/DD HH:MM:SS" که میلادی است.
 - invoice_date: تاریخ فاکتور که با فرمت دلخواه فروشگاه است.
 - invoice_number: شماره ی فاکتور
 - merchant_code: شماره ی فروشگاه نزد درگاه پرداخت امن پاسارگاد
 - terminal_code: شماره ی ترمینال فروشگاه نزد درگاه پرداخت امن پاسارگاد
 - redirect_address: آدرس فروشگاه که در صورت موفقیت آمیز بودن عملیات، مشتری از سیستم پرداخت امن به آنجا فرستاده خواهد شد. پارامترهای ارسالی به این صفحه شامل تاریخ فاکتور در فیلد id، شماره ی فاکتور در فیلد iN و شماره ی رسیدی که به مشتری نمایش داده می شود در فیلد tref است.
 - referrer_address: آدرس فروشگاه که در صورت لغو خرید، مشتری به آنجا فرستاده خواهد شد.
 - delivery_days: تعداد روزهایی است که فروشنده زمان دارد تا کالا را به دست خریدار برساند. این تعداد به صورت کلی و برای همه ی کالاهای یک فاکتور در نظر گرفته می شود.
 - total_amount: مقدار ارزش ریالی فاکتور است که خریدار باید آنرا در ازای خرید خود بپردازد.
 - buyer_name: نام خریدار که باید توسط فروشگاه به درگاه پرداخت امن فرستاده شود.
 - buyer_tel: شماره تلفن تماس خریدار که باید توسط فروشگاه به درگاه پرداخت امن فرستاده شود.
 - delivery_address: آدرس تحویل کالاها که باید توسط فروشگاه به درگاه پرداخت امن فرستاده شود.
 - Timeout: مهلت پرداخت فاکتور و تکمیل خرید.
- اطلاعات مربوط به کالاهای موجود در فاکتور، به صورت جداگانه برای هر کالا در یک المان `<item />` فرستاده می شود. هر کالا دارای یک شماره ردیف است که در فیلد number در المان item مشخص می شود. این شماره از یک شروع شده و با اضافه شدن کالای جدید بالا می رود. در ضمن زمان رخداد و شماره رخداد هر رقم کالا تیترا داخل این المان در فیلدهای event_date و event_id مشخص می شود. بقیه ی فیلدهای ارسالی برای هر کالا به شرح زیر است:
 - content: محتوای در نظر گرفته شده برای هر کالا که شامل نام کالا یا چیزی شبیه به آن است.
 - fee: قیمت واحد کالا.
 - count: تعداد موجود از کالا در فاکتور.
 - description: توضیحات مربوط به کالا که می تواند شرح مختصری از خصوصیات آن باشد.
 - cancel: در این المان اطلاعات مربوط به عمل لغو مشخص می شود. در فیلد from در المان cancel زمان آغازی که قانون اعمال می شود به دو فرمت تاریخ مطلق به صورت "YYYY/MM/DD HH:MM:SS" که میلادی است و تاریخ نسبی به صورت "M یا D یا H تعداد ماه یا روز یا ساعت ±" به نسبت تاریخ رویداد مشخص می شود. مانند "+2D" به معنای دو روز بعد از تاریخ رویداد و یا "12H-" به معنای ۱۲ ساعت قبل از تاریخ رویداد. سایر اطلاعات مربوط به عمل لغو به در فیلدهای زیر مشخص می شود.
 - percent: درصد سهم مشتری از مبلغ کالا (عدد بین ۰ تا ۱۰۰)
 - constant: سهم مشتری به صورت ثابت (مستقل از مبلغ کالا)

clearing: این قسمت مربوط به مالتی مرچنت ها است. دارای المان deposit است و در هر المان فیلد code شناسه حساب را مشخص میکند. عدد داخل تگ clearing مشخص کننده سهم هر مرچنت است.

دریافت نتیجه تراکنش

برای دریافت نتیجه تراکنش، سایت فروشنده باید رسید دریافتی از درگاه در پارامتر tref را، به صورت POST به آدرس نسبی /PaymentTrace ارسال کند. نتیجه به صورت XML در پاسخ در خواست ارسال می شود. نمونه ی این XML در زیر آمده است. بدیهی است که result، نشان دهنده موفقیت آمیز بودن تراکنش است. در صورت موفقیت انجام تراکنش، trace_number، reference_number و transaction_date به ترتیب شماره ی پیگیری، شماره ارجاع و تاریخ تراکنش می باشد. در غیر این صورت، مقادیر این داده ها نامعتبر می باشد. اگر سایت فروشنده به هر دلیل موفق به دریافت مقدار پارامتر tref نشده باشد، می تواند با فرستادن داده های invoice_date، invoice_number، merchant_code و terminal_code به همان آدرس به صورت POST، از نتیجه تراکنش، به صورت گفته شده، باخبر شود. نیازی به توضیح نیست که داده های ارسالی باید در پارامترهای گفته شده قرار بگیرند و رعایت کوچک و بزرگ بودن حروف الزامی می باشد و نیز ترتیب ارسال پارامترها در درخواست ارسالی، بی اهمیت است.

```
<result_obj>
  <result>{true|false}</result>
  <transaction_reference_id>tref</transaction_reference_id>
  <invoice_number>شماره فاکتور</invoice_number>
  <invoice_date>تاریخ فاکتور</invoice_date>
  <merchant_code>شماره فروشگاه</merchant_code>
  <terminal_code>شماره ترمینال فروشگاه</terminal_code>
  <trace_number>شماره پیگیری</trace_number>
  <reference_number>شماره ارجاع</reference_number>
  <transaction_date>تاریخ تراکنش</transaction_date>
</result_obj>
```

شکل دو، XML نشان دهنده ی نتیجه ی یک تراکنش انجام شده در درگاه امن