



Saman Micro Payment

Technical Specification

Last update at: August 2014

هدف این نوشته

این نوشته قدم‌های لازم برای ایجاد بستر پرداخت با استفاده از رسید دیجیتالی را در سمت فروشنده بر می‌شمارد. ساختار این نوشته به صورت ذیل است:

۱. تعریف اجزای سیستم

اجزای مربوط به خریدار
اجزای مربوط به فروشنده
اجزای مربوط به پرداخت الکترونیک سامان

۲. نیازمندی‌های امنیتی و بانکی

نیازمندی‌های امنیتی
نیازمندی‌های بانکی

۳. بسترسازی سمت فروشنده

انجام تراکنش
پشتیبانی مشتریان

ضمیمه‌ها

الف. تکنولوژی‌های مورد استفاده

استفاده از Web service ها

ب. شرح متدها

تابع تایید
تابع برگشت
شرح خطاها

پ. پارامترهای تبادلی میان سایت فروشنده و سایت پرداخت الکترونیک سامان

پارامترهای دریافتی از فروشنده
پارامترهای ارسالی به فروشنده

۱. تعریف اجزای سیستم

سیستم پرداخت الکترونیکی، از اجزاء زیر تشکیل شده است:

خریدار

- خریدار: موجودیتی که تقاضای خرید سرویس یا کالا دارد.
- کارت: موجودیتی برای برداشت و خرید در فروشگاه یا اینترنت توسط خریدار.

فروشنده

- فروشنده: موجودیتی که سرویس یا کالا را در اختیار خریدار قرار می‌دهد.
- کد فروشنده (Merchant ID): یا کد پذیرنده که شامل کدی است که توسط پرداخت الکترونیک سامان به فروشنده اختصاص می‌یابد.

پرداخت الکترونیک سامان

- تراکنش (Transaction): یک عملیات مالی، که در این مستند یک خرید اینترنتی است.
- سایت پرداخت الکترونیک سامان: سایتی متعلق به پرداخت الکترونیک سامان است که در آن خریدار مشخصات کارت و رمز آن را وارد می‌نماید و انتقال مبلغ خرید به سپرده فروشنده را تایید می‌کند و در صورت موفقیت‌آمیز بودن انتقال، یک رسید دیجیتالی برای آن تراکنش صادر می‌شود (در واقع این کار می‌تواند به عنوان بخشی از وظایف ماشین پذیرنده در نظر گرفته شود).
- رسید دیجیتالی (Reference Number): رسید دیجیتالی یا RefNum یک رشته‌ی حداکثر ۵۰ کاراکتری که سایت پرداخت الکترونیک سامان به عنوان رسید پس از انجام تراکنش موفق به فروشنده و خریدار ارائه می‌دهد. این رشته به صورت UNIQUE در سطح سیستم تولید می‌شود.
- شماره خرید (Reservation Number): شماره خرید یا ResNum کدی که فروشنده برای هر تراکنش خریدار در نظر می‌گیرد و خریدار می‌تواند توسط آن کد، خرید خود را پیگیری کند (در واقع مشخصه تراکنش، شماره خرید، شماره ی فاکتور و غیره در سمت فروشنده است).

۲. نیازمندی‌های امنیتی و بانکی

قبل از پرداختن به موضوع نیازمندیها احتیاج به تعریف گواهینامه امنیتی (SSL certificate) است. گواهینامه امنیتی یک نوع روش کدگذاری (Encryption) آنلاین به روی تمامی اطلاعات و فایل‌هایی است که مابین وب سایت و کاربر رد و بدل می شود. این نوع کدگذاری بالاترین سطح امنیت در اینترنت برای انتقال داده ها است. در این نوع روش برای امن کردن داده ها روی وب هنگام صدا زدن وب سایت مورد نظر از پروتکل https (Secure http) به معنای وب امن به جای http استفاده می شود. به طور مثال با آدرس <http://sep.shaparak.ir> اطلاعات به صورت غیر کدشده و معمولی رد و بدل می شود در حالی که با آدرس <https://sep.shaparak.ir> اطلاعات به صورت کدشده مابین وب سایت و کاربر رد و بدل می شود. لازم به ذکر است که وب سایتهایی این قابلیت را دارا هستند که گواهینامه امنیتی خود را از مراکز صدور این گواهینامه ها تهیه کرده و روی وب سایت خود نصب کرده باشند.

نیازمندی‌های امنیتی

سایتهای پرداخت الکترونیک سامان (sep.shaparak.ir و www.samanepay.com) دارای گواهینامه های امنیتی معتبر بوده و ارتباط خریدار با پرداخت الکترونیک سامان، همچنین فروشنده با پرداخت الکترونیک سامان می تواند در بستر SSL انجام شود. این آماده سازی از قبل توسط پرداخت الکترونیک سامان انجام گرفته است تا تراکنش در بستر امن صورت پذیرد. اگر فروشنده نیز دارای گواهینامه معتبری باشد، ارتباط بین خریدار و فروشنده نیز در بستر SSL و به صورت امن خواهد بود. اینکه فروشنده دارای گواهینامه معتبر باشد، اجباری نیست، بلکه بهتر است اینگونه باشد.

نیازمندی امنیتی دیگر این است که فروشنده از هیچ کدام از اطلاعات مالی خریدار (مانند مشخصات کارت، رمز کارت، میزان موجودی و) مطلع نشود. به همین خاطر فروشنده از خریدار هیچ نوع اطلاعات مالی و بانکی دریافت نمی کند و تمامی این اطلاعات توسط خریدار در سایت پرداخت الکترونیک سامان وارد می شود.

نیازمندی امنیتی دیگر این است که فقط فروشنندگان مجاز قادر باشند که درخواست تایید یک تراکنش را صادر کنند. این امر با قرار دادن یک فایروال جلوی ماشین پذیرنده (Acquirer) محقق شده است و آدرس IP فروشنده باید به پرداخت الکترونیک سامان داده شود، تا اجازه دسترسی برای آن صادر شود.

کلمه رمزی به فروشنده داده می شود. این کلمه رمز در هنگام راه اندازی فروشنده برای بار اول از طرف پرداخت الکترونیک سامان به فروشنده داده و جهت مشاهده تراکنش ها در وب سایت گزارش دهی پرداخت الکترونیک سامان و نیز برگشت تراکنش مورد استفاده دارد.

نیازمندی‌های بانکی

فروشنده باید سپرده ای را نزد یکی از شعب بانک افتتاح نماید و آن را به عنوان "سپرده فروشنده" به پرداخت الکترونیک سامان معرفی نماید. پرداخت الکترونیک سامان نیز به وی

یک کد پذیرنده (Merchant ID) اختصاص خواهد داد که در هر تراکنش فروشنده خود را با ارائه این کد به پرداخت الکترونیک سامان معرفی می‌کند.

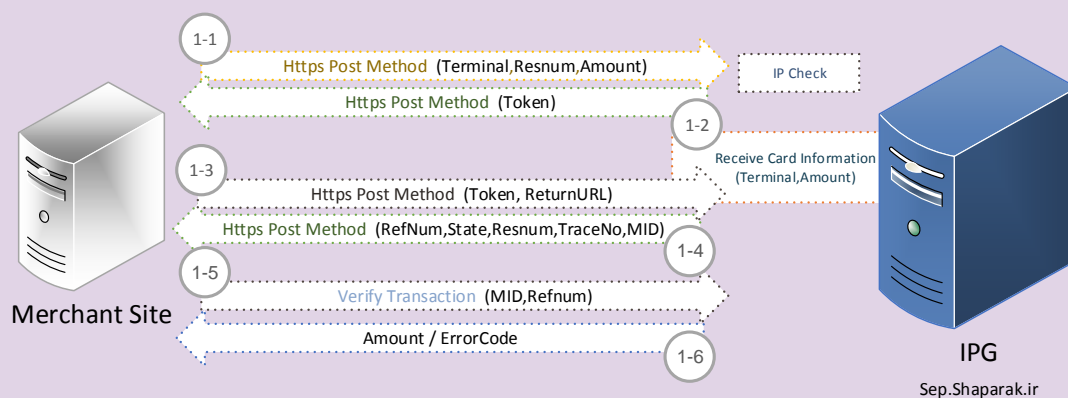
۳. بسترسازی سمت فروشنده

در حال حاضر دو سناریو، برای استفاده از درگاه پرداخت اینترنتی سامان توسط فروشنده و تکمیل فرآیند خرید وجود دارد که این دو سناریو در ادامه بخش ۳ (همین بخش) شرح داده شده‌اند. سناریوی اول، ارسال مستقیم اطلاعات خرید مشتری به وب سایت درگاه پرداخت اینترنتی پرداخت الکترونیک سامان به منظور انجام تراکنش، روی بستر امن (https) است که در این سناریو، همزمان با ارسال اطلاعات، خریدار به وبسایت درگاه پرداخت اینترنتی هدایت می‌شود. سناریوی دوم، ارسال اطلاعات خرید مشتری به وب سرویس دریافت توکن درگاه پرداخت اینترنتی پرداخت الکترونیک سامان به منظور دریافت توکن در مرحله اول و ارسال توکن به وب سایت درگاه پرداخت اینترنتی به منظور انجام تراکنش در مرحله دوم است که هر دو مرحله سناریوی دوم روی بستر امن (https) انجام می‌شود. در این سناریو، تا زمان دریافت توکن از درگاه پرداخت اینترنتی، کاربر به سمت درگاه پرداخت اینترنتی هدایت نمی‌شود.

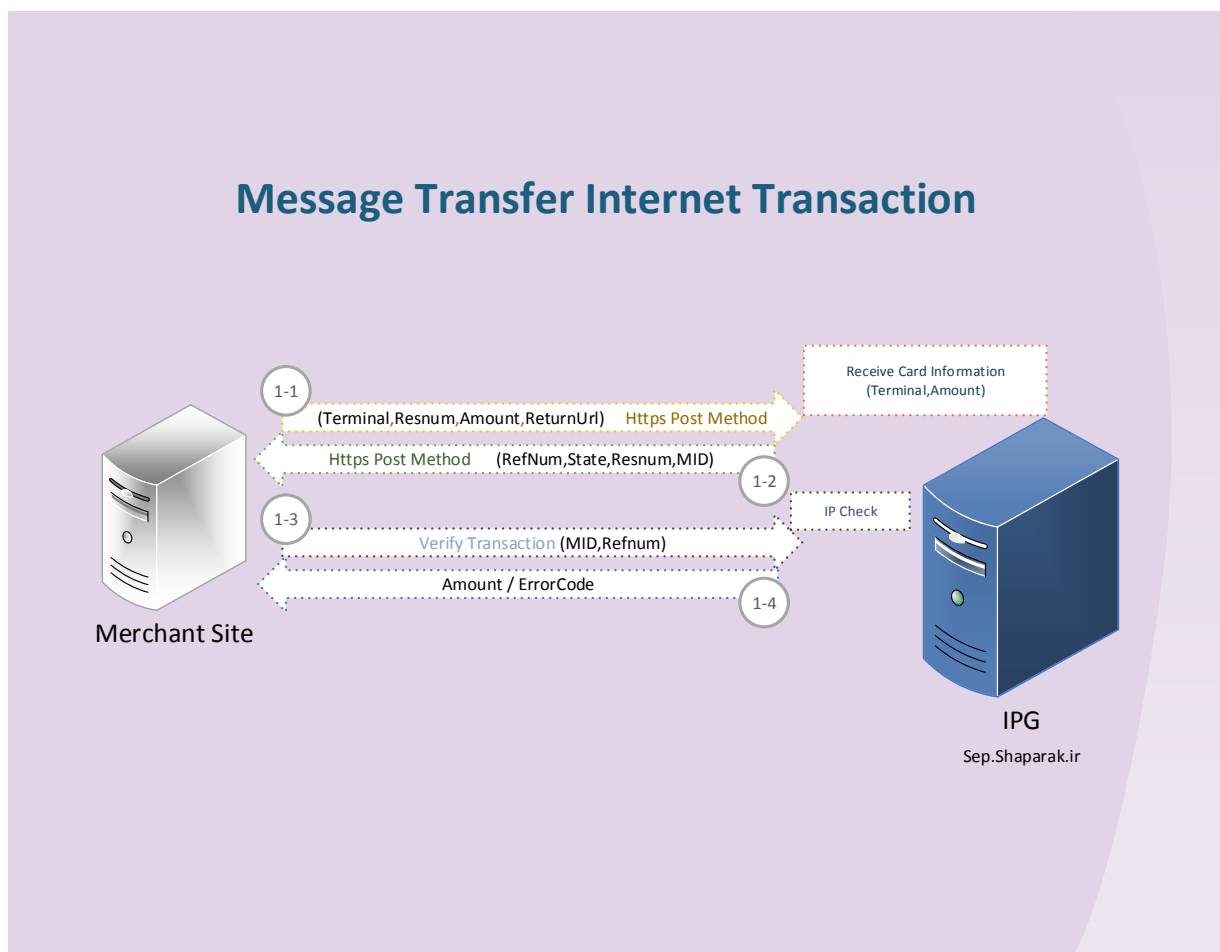
سناریوی دوم نسبت به سناریوی اول، یک رفت و برگشت بین وب سایت فروشنده و درگاه پرداخت اینترنتی پرداخت الکترونیک سامان، به مراحل تبادل اطلاعات اضافه می‌کند، و در عین حال، امنیت بیشتری دارد.

شکل‌های ۱ و ۲ فرآیند کلی این دو سناریو را نشان می‌دهد.

Message Transfer Internet Transaction



شکل ۱ . سناریوی انجام فرآیند پرداخت با استفاده از توکن



شکل ۲. سناریوی انجام فرآیند پرداخت بدون استفاده از توکن

انجام تراکنش

فروشنده خریدار را به نقطه‌ای می‌رساند که آماده دریافت پول و نهایی کردن خرید است. این نقطه می‌تواند در انتهای روال خرید از طریق یک سبد خرید، نهایی کردن خرید یک بلیط و موارد مشابه باشد. در این نقطه فروشنده باید مراحل زیر را دنبال نماید (نکته: مراحل ۱ تا ۴ برای هر دو سناریو یکسان نیست (مراحل ۱ تا ۳ مخصوص سناریوی اول و مرحله ۴ مخصوص سناریوی دوم می‌باشد) و با توجه به سناریوی مورد ترجیح فروشنده، گام‌های مورد نیاز باید طی شود؛ اما گام‌های ۴ به بعد در هر دو سناریو مشترک است):

۱. فروشنده، به منظور انجام تراکنش و هدایت خریدار به وب سایت پرداخت

الکترونیک سامان، وب سرویس دریافت توکن را فراخوانی می‌کند (نکته: این گام

مخصوص سناریوی ارجاع خریدار به صفحه پرداخت با استفاده از توکن

(سناریوی اول) می‌باشد):

فروشنده به منظور هدایت خریدار به وب سایت پرداخت الکترونیک سامان و

انجام فرآیند مالی، متد وب سرویس دریافت توکن به نام RequestToken را

فراخوانی می‌کند. برای این منظور، فروشنده باید پارامترهای زیر را به عنوان پارامتر الزامی با استفاده از متد POST به وب سرویس ارسال کند:

i. مبلغ تراکنش: TotalAmount

ii. کد پذیرنده: TermID

iii. شماره خرید: ResNum

TotalAmount: مبلغ تراکنش خرید است که فروشنده می‌خواهد از خریدار دریافت نماید. این اطلاعات باید به صورت یک عدد صحیح (long) باشد و از هرگونه کاراکتر غیر عددی مانند نقطه (.) پرهیز شود. در صورتی که مبلغ از نوع integer نباشد، صفحه ی پرداخت خطا تولید می‌کند (این امر به خصوص در هنگام استفاده از سیستم های فروشگاه های آماده به ویژه سیستم هایی که در خارج از ایران آماده شده اند باید مورد توجه قرار گیرد).
TermID: کد پذیرنده است که برای شناسایی فروشنده در هر تراکنش لازم است.

ResNum: شماره خرید یا شماره فاکتور خرید مشتری در وب سایت فروشنده است. از دید پرداخت الکترونیک سامان، نیازی به یکتا (Unique) بودن شماره فاکتور خرید وجود ندارد. (یکتا بودن شماره خرید از طرف پرداخت الکترونیک سامان، کنترل نمی‌گردد و اگر این امر برای فروشنده مهم است، می‌بایست در سیستم خود این موضوع بررسی شود).
فروشنده باید از شماره خرید (ResNum) به جای session و cookie برای تعقیب رفت و برگشت خریدار به وب سایت پرداخت الکترونیک سامان استفاده کند.

آدرس وب سرویس پرداخت الکترونیک سامان برای ارسال پارامترها و دریافت توکن <https://sep.shaparak.ir/Payments/InitPayment.aspx> است. همانطور که مشاهده می‌شود این وب سایت از پروتکل وب امن و گواهینامه امنیتی استفاده می‌کند.

شرح کامل پارامترهای اجباری و اختیاری که فروشنده در اختیار پرداخت الکترونیک سامان می‌گذارد در ضمیمه پ آورده شده است.

۲. وب سرویس پرداخت الکترونیک سامان، توکن را برای فروشنده ارسال می‌کند
(**نکته: این گام مخصوص سناریوی ارجاع خریدار به صفحه پرداخت با استفاده از توکن (سناریوی اول) می‌باشد:**)

وب سرویس پرداخت الکترونیک سامان (متد RequestToken)، پس از دریافت کد پذیرنده، شماره خرید و مبلغ، توکن مربوط به تراکنش را برای فروشنده ارسال می‌کند.

۳. فروشنده، با ارسال توکن دریافتی به همراه آدرس URL بازگشتی (صفحه ی callback) با استفاده از متد POST، خریدار را به وبسایت پرداخت

الکترونیک سامان هدایت می‌کند (نکته: این گام مخصوص سناریوی ارجاع خریدار به صفحه پرداخت با استفاده از توکن (سناریوی اول) می‌باشد).

خریدار به وب سایت پرداخت الکترونیک سامان هدایت (Redirect) می‌شود. مواردی که به صفحه ی پرداخت به صورت متد POST ارسال می‌شود عبارتند از:

- i. توکن دریافتی: Token
- ii. آدرس بازگشتی RedirectURL

Token: توکنی که فروشنده در مرحله نخست از پرداخت الکترونیک سامان دریافت کرده است.

RedirectURL: آدرس بازگشتی شامل آدرسی است در وب سایت فروشنده که اطلاعات تراکنش از سمت سایت پرداخت الکترونیک سامان به آن ارسال می‌شود.

آدرس سایت پرداخت الکترونیک سامان برای ارسال پارامترها <https://sep.shaparak.ir/Payment.aspx> است. همانطور که مشاهده می‌شود این وب سایت از پروتکل وب امن و گواهینامه امنیتی استفاده میکند. شرح کامل پارامترهای اجباری و اختیاری که فروشنده در اختیار پرداخت الکترونیک سامان می‌گذارد در ضمیمه پ آورده شده است.

۴. فروشنده , خریدار را به وب سایت پرداخت الکترونیک سامان هدایت می‌کند: (نکته: این گام مخصوص سناریوی ارجاع خریدار به صفحه پرداخت بدون استفاده از توکن (سناریوی دوم) می‌باشد)

خریدار به وب سایت پرداخت الکترونیک سامان هدایت (Redirect) می‌شود. مواردی که به صفحه ی پرداخت به صورت متد POST ارسال می‌شود عبارتند از:

- i. مبلغ تراکنش: Amount
- ii. کد پذیرنده: MID
- iii. شماره خرید: ResNum
- iv. آدرس بازگشتی RedirectURL

Amount: مبلغ تراکنش خرید است که فروشنده می‌خواهد از خریدار دریافت نماید. این اطلاعات باید به صورت یک عدد صحیح (integer) باشد و از هرگونه کاراکتر غیر عددی مانند نقطه (.) پرهیز شود. در اینصورت صفحه ی پرداخت خطا تولید می‌کند. (این امر به خصوص در هنگام استفاده از سیستم های فروشگاه‌های آماده به ویژه سیستم هایی که در خارج از ایران آماده شده اند باید مورد توجه قرار گیرد).

MID: کد فروشنده است که برای شناسایی فروشنده در هر تراکنش لازم است. ResNum: شماره خرید یا شماره فاکتور خرید مشتری در وب سایت فروشنده

است. از دید پرداخت الکترونیک سامان، نیازی به یکتا (Unique) بودن شماره فاکتور خرید وجود ندارد.

فروشنده باید از شماره خرید (ResNum) بجای session و cookie برای تعقیب رفت و برگشت خریدار به وب سایت پرداخت الکترونیک سامان استفاده کند.

RedirectURL: آدرس بازگشتی شامل آدرسی است در وب سایت فروشنده که اط به آن ارسال می شود. لاعات تراکنش از سمت سایت پرداخت الکترونیک سامان

آدرس سایت پرداخت الکترونیک سامان برای ارسال پارامترها <https://sep.shaparak.ir/Payment.aspx> است. همانطور که مشاهده می شود این وب سایت از پروتکل وب امن و گواهینامه امنیتی استفاده میکند. شرح کامل پارامترهای اجباری و اختیاری که فروشنده در اختیار پرداخت الکترونیک سامان می گذارد در ضمیمه پ آورده شده است.

۵. خریدار مشخصات کارت و رمز آن را در فرم مخصوص وارد می کند : در وب سایت پرداخت الکترونیک سامان ، خریدار اطلاعات کارت خود، شامل موارد زیر را وارد می کند:

- i. شماره کارت (PAN)
- ii. کلمه عبور دوم (رمز خرید اینترنتی) (PIN II)
- iii. تاریخ انقضای کارت (Expire Date)
- iv. CVV2

توجه : دریافت این اطلاعات از خریدار، در وب سایت پرداخت الکترونیک سامان پیاده سازی شده و فروشنده نیازی به انجام توسعه برای این منظور ندارد.

۶. وب سایت پرداخت الکترونیک سامان خریدار را به وب سایت فروشنده هدایت می کند: وب سایت پرداخت الکترونیک سامان پس از اتمام تراکنش، خریدار را دوباره به سایت فروشنده به آدرس RedirectURL هدایت می کند (Redirect می کند). فروشنده پارامترهای پاس شده از وب سایت پرداخت الکترونیک سامان را با متد POST دریافت می کند. پارامترهای ارسالی عبارتند از:

- i. State (وضعیت تراکنش)
- ii. RefNum (رسید دیجیتالی خرید)
- iii. ResNum (شماره خرید)
- iv. MID (کد پذیرنده)
- v. TraceNo (کد رهگیری)

فروشنده می‌تواند بر اساس وضعیت تراکنش، موفقیت‌آمیز بودن تراکنش را تشخیص دهد. شرح کامل پارامترها در ضمیمه پ آورده شده است.

۷. فروشنده وضعیت تراکنش را تشخیص داده و آن را چک می‌کند؛ از روی فیلد وضعیت تراکنش STATE، فروشنده می‌تواند متوجه شود که آیا پرداخت موفقیت‌آمیز بوده است یا خیر (مقدار دقیق این فیلد و نحوه تصمیم‌گیری روی آن در ضمیمه پ آورده شده است). اگر خرید موفقیت‌آمیز نبود فروشنده موظف است خطای به وجود آمده و علت آن را با توجه به فیلد وضعیت تراکنش برای خریدار شرح دهد. اگر وضعیت تراکنش OK بود، فروشنده رسید دیجیتالی (RefNum) را در پایگاه داده خود جستجو می‌کند. این کار به منظور جلوگیری از Double Spending یا دوبار مصرف شدن یک رسید دیجیتالی است. این مسئله کاملاً به عهده فروشنده است زیرا این رسید دیجیتالی به صورت منحصر به فرد (Unique) از طرف پرداخت الکترونیک سامان صادر می‌شود و پرداخت الکترونیک سامان در برابر دو بار مصرف شدن رسید دیجیتالی سمت سایت فروشنده هیچ عکس‌العملی را نشان نمی‌دهد (به بیان دیگر اگر یک رسید دیجیتالی جهت تایید بیش از یک بار به پرداخت الکترونیک سامان ارائه شود، پرداخت الکترونیک سامان مجدداً آن را تایید می‌کند). توجه داشته باشید که ممکن است یک مشتری رسید دیجیتالی صادر شده توسط پرداخت الکترونیک سامان را ذخیره نماید و به ازای یک خرید دیگر از آن استفاده کند. در این زمان فروشنده باید تمهیدات لازم را سمت خود پیاده‌سازی کرده باشد تا برای دو خرید متفاوت، از یک رسید دیجیتالی واحد استفاده نشود. همانگونه که قبلاً ذکر شد اینکار با ذخیره رسید دیجیتالی در بانک اطلاعاتی فروشنده و مقایسه رسید دیجیتالی جدید با رسیدهای موجود از قبل در بانک اطلاعاتی، قابل انجام است. در صورت عدم وجود رسید دیجیتالی در بانک اطلاعاتی فروشنده، فروشنده، Verify Web Method را با پارامترهای زیر صدا می‌زند:

i. RefNum
ii. MID

فروشنده باید این متد را صدا بزند و به نتیجه دریافتی از تراکنش اکتفا ننماید، در غیر این صورت، حتی اگر نتیجه انجام تراکنش اولیه موفق بوده باشد ولی تراکنش از سمت فروشنده در مدت زمان ۳۰ دقیقه، verify نشود، تراکنش به صورت خود به خود برگشت زده می‌شود و پول به حساب خریدار بازگردانده می‌شود. مقدار برگشتی این تابع باید برابر مقدار کل خرید (Amount) باشد و در غیر این صورت تراکنش دارای مشکل است. با مقایسه این مبلغ و مبلغ فاکتوری که فروشنده خود در اختیار دارد ۳ حالت زیر ممکن است به وجود آید:

A. اگر خروجی تابع مثبت و برابر مبلغ درخواستی فروشنده باشد، فروشنده میتواند سرویس خود را ارایه دهد (مرحله ۵).

B. اگر این دو مبلغ برابر نباشند، کل مبلغ باید به حساب مشتری

بازگردانده شود و فروشنده نباید سرویس خود را ارایه نماید.

C. خروجی این تابع اگر منفی باشد بیانگر رویداد خطایی می باشد که

شرح این خطاها نیز در ضمیمه ب آورده شده است.

نکته مهم: توجه فرمایید که تنها در حالت A خرید موفقیت آمیز بوده و فروشنده

باید کالا یا خدمات مربوطه را به مشتری ارائه نماید.

شرح کل این تابع نیز در ضمیمه ب آمده است.

۸. **تکمیل روند خرید:** در صورت درست بودن تراکنش، فروشنده رسید دیجیتالی

را در رکورد مربوط به آن ResNum (که قبل از تراکنش به عنوان یک پارامتر

به پرداخت الکترونیک سامان پاس داده شده و بعد از تراکنش وب سایت

پرداخت الکترونیک سامان به فروشنده پاس داده است) در پایگاه داده خود

ذخیره می کند. در صورت درست نبودن مبلغ انتقالی نیز رسید دیجیتالی ذخیره

می شود تا خریدار بتواند درخواست برگشت آن را به فروشنده ارائه دهد.

نکات:

الف) دوباره تاکید می شود که مصرف شدن رسید دیجیتالی در سمت فروشنده تعیین و

نگهداری می شود و نه در سمت پرداخت الکترونیک سامان. پرداخت الکترونیک سامان

تنها اعتبار و مبلغ برگشت نخورده رسید دیجیتالی را گزارش می دهد. بدین ترتیب

پرداخت الکترونیک سامان می تواند مشخصات یک رسید دیجیتالی را چندین بار به

فروشنده گزارش دهد بدون آن که وضعیت مصرف شدگی آن تغییر کند. حسن این روش

در این است که اگر فروشنده ای یک رسید دیجیتالی را برای اعتبارسنجی به پرداخت

الکترونیک سامان بدهد و پرداخت الکترونیک سامان نیز نتیجه را برای فروشنده ارسال

دارد ولی این جواب به هر دلیلی به دست فروشنده نرسد، رسید دیجیتالی اعتبار خود را

از دست نخواهد داد و فروشنده می تواند دوباره تقاضای اعتبارسنجی نماید و در صورت

مثبت بودن نتیجه آن را در پایگاه داده خود ذخیره کرده و وضعیت رسید تراکنش را به

مصرف شده تغییر دهد. **اما به لحاظ امنیتی باید فروشنده مراقب باشد تا از یک رسید**

دیجیتالی برای دو خرید متفاوت استفاده نشود. این امر به خصوص در هنگام ارائه

خدمات (از قبیل فروش شارژ کارت تلفن همراه، کارت اینترنت و ...) حائز اهمیت است.

ب) در صورتی که جواب تابع verifyTransaction به هر دلیلی به دست فروشنده نرسد

(Timeout شود، مشکل شبکه پیش آمده باشد و ...) فروشنده باید به تعداد مشخصی

مجددا سعی نماید. دقت شود تکرار در صورتی باید انجام شود که جواب به دست

فروشنده نرسد، نه اینکه نتیجه verifyTransaction نشان دهنده خطا باشد (منفی

باشد).

ت) در صورتی که تراکنش به هر دلیلی در مدت زمان مشخصی (در حال حاضر حداکثر ۳۰

دقیقه) از جانب فروشنده تایید نشد، پرداخت الکترونیک سامان اقدام به برگشت زدن

تراکنش خواهد کرد و پول به حساب خریدار برگردانده می شود.

ث) در این روش پرداخت، امکان اینکه یک رسید دیجیتالی توسط دو فروشنده‌ی مختلف استفاده شود، وجود ندارد؛ این مساله سمت پرداخت الکترونیک سامان و با توجه به شماره IP و کد پذیرنده کنترل خواهد شد.

ج) مسئولیت جلوگیری از Double Spending بر عهده فروشنده است و در صورت ضعفی در پیاده‌سازی سایت فروشنده، ضرر آن متوجه خود اوست و پرداخت الکترونیک سامان، هیچ گونه مسئولیتی در قبال موارد Double Spending نخواهد داشت.

ح) امنیت این بخش از سیستم به کمک SSL و ACL تامین شده است.

خ) مدیریت ریسک این بخش با استفاده از سقف‌های برداشت برای موجودیت خریدار و الگوهای فروش برای فروشنده صورت می‌گیرد. خریدار با تعیین سقف انتقال سپرده‌های خود می‌تواند میزان ریسک سپرده‌های خود را مدیریت نماید. همچنین فروشنده با معرفی الگوی فروش خود به پرداخت الکترونیک سامان، حداکثر مبالغ فروش خود را معرفی می‌نماید.

د) چک کردن IP فروشنده تنها در زمان فراخوانی web service پرداخت الکترونیک سامان انجام می‌شود، در مرحله اول که مشتری از سایت فروشنده به سایت پرداخت الکترونیک سامان منتقل می‌شود، هیچ کنترلی بر روی IP فروشنده صورت نمی‌گیرد. **در صورتی که با پیغام فروشنده نزد بانک شناخته شده نیست مواجه شدید، یا شماره MID و یا سایر اطلاعات را به اشتباه ارائه کرده‌اید.**

:Online Demo

برای مشاهده online demo یک سناریوی ساده پرداخت، به آدرس <http://demo.sep.ir> مراجعه کنید.

:Sep IMS

برای مشاهده online لیست تراکنشهای صورت گرفته در هر روز می‌توانید به آدرس <https://acquirer.samanepay.com/Merchants> مراجعه نمایید (برای ورود به این سیستم نیاز به داشتن کلمه عبور است که جهت دریافت آن باید با بخش فنی تماس بگیرید).

پشتیبانی مشتریان

از آنجا که سایت شما در حال ارائه خدمات ۷*۲۴ (شبانه روزی) است، بنابراین ایجاب می‌کند که پشتیبانی از طریق یک نقطه تماس فیزیکی ۷*۲۴ نیز در سایت شما تعیبه گردد. این نقطه تماس که می‌تواند شامل تلفن و Email باشد لازم است به صورت واضح و آشکار در وب سایت فروشنده نمایش داده شود.

ضمیمه ها

الف : تکنولوژی‌های مورد استفاده

برای پیاده سازی این سیستم از تکنولوژی Web Services استفاده شده است و ارتباطی نقطه به نقطه بین سایت فروشنده و پرداخت الکترونیک سامان برقرار می‌گردد. در این مدل سرویس‌هایی که از جانب پرداخت الکترونیک سامان ارائه می‌شود در قالب توابعی در اختیار فروشنده قرار می‌گیرد تا در سایت خود از آنان استفاده نماید. فروشنده می‌تواند این توابع را به صورت مسقیم از متن برنامه‌ی سایت خود صدا بزند. انتقال اطلاعات در لایه پایین‌تر مطابق پروتکل SOAP^۱ خواهد بود. خود پروتکل SOAP برای دسته بندی و مدیریت داده‌ها از استاندارد XML استفاده می‌کند. در لایه ترانسپورت نیز انتقال داده‌ها بر عهده پروتکل HTTP و یا HTTPS می‌باشد. حسن استفاده از Web Services در این است که فروشنده می‌تواند از هر تکنولوژی‌ای برای پیاده‌سازی سایت خود استفاده نماید. مثال‌هایی از نحوه consume کردن و فراخواندن این web method ها برای عموم تکنولوژی‌های موجود تهیه شده است و فروشنده می‌تواند از آنان برای سایت خود بهره گیرد.

استفاده از Web Method ها:

- برای استفاده از هر یک از Web Method ها تحت تکنولوژی PHP ۴، باید ابتدا PHP Module ی را به نام NuSOAP به سیستم فروشنده اضافه نمایید و مسیر آن را در کد خود (مطابق نمونه کد داده شده) مشخص نمایید.
- برای استفاده از web service تحت تکنولوژی PHP 5، از آنجا که در این نسخه از PHP پشتیبانی از پروتکل SOAP افزوده شده است، چنانچه ماژول های SOAP برای PHP فعال شده باشد (در هنگام کامپایل تحت لینوکس و یا با فعال سازی DLL مربوطه در سیستم عامل ویندوز)، نیازی به استفاده از NuSOAP نیست و از کد های مربوط به PHP 5 باید استفاده شود. در صورتی که مایل به استفاده از NuSOAP تحت PHP 5 هستید، باید در فایل nusoap.php و نیز تمام فایل های دیگری که از آن استفاده می کنند، تابع soapclient را به نام دیگری rename کنید.
- تحت تکنولوژی ASP (و به طور کلی برای استفاده از web service تحت سیستم عامل ویندوز) باید ابتدا SOAPSDK را بر روی سیستم فروشنده نصب نمایید. این SDK را می‌توانید از <http://www.microsoft.com/downloads> دریافت نمایید. روش استفاده از آن در نمونه کدها آمده است.
- در تکنولوژی ASP .NET می‌توان از پشتیبانی خود .NET برای صدا زدن Web Method استفاده کرد. روش استفاده در نمونه کد آورده شده است.

^۱ Simple Object Access Protocol

- در تکنولوژی دلفی نیز می توان از پشتیبانی خود زبان برنامه نویسی استفاده کرد (البته در نسخه های خاصی از دلفی این پشتیبانی وجود دارد). اگر نسخه دلفی شما Web Service را به صورت محلی پشتیبانی نمی کند، می توان از بسته نرم افزاری SOAPSDK استفاده نمایید. SOAPSDK به صورت یک ActiveX در می آید که در اکثر زبانهای برنامه نویسی می توان از آن استفاده کرد. نمونه کد دلفی برای هر دو حالت موجود است.
- در تکنولوژی Perl استفاده از بسته نرم افزاری SOAP-Lite توصیه می شود. نمونه کد صدا زدن وب متدها موجود است.
- برای تکنولوژی جاوا یک wrapper بر روی interface متدها ایجاد شده است به نام client.jar که باید آن را (به همراه دیگر jar های مرتبط با استفاده از Web Services) در classpath خود قرار دهید.

ب: شرح Web Methods

تابع (Web Method) در اختیار فروشندگان قرار می‌گیرد که شرح پارامترهای ورودی و خروجی آن در ذیل آمده است. توجه داشته باشید که نام type مقادیر ورودی و برگشتی، نام‌های عامی می‌باشند که در هر زبان برنامه‌نویسی ممکن است تفاوت یابند. همچنین مقدار برگشتی تابع با نام خود آن تابع مشخص شده است.

۱- تابع تایید یک تراکنش

```
double verifyTransaction (
    String RefNum,
    String MerchantID)
```

پارامترهای ورودی تابع

پارامتر	نوع	توضیحات
RefNum	String	شماره رسید دیجیتالی‌ای که مایل به تایید آن توسط پرداخت الکترونیک سامان هستید. این کد باید از ۲۰ تا ۵۰ کاراکتر باشد.
MerchantID	String	کد فروشنده. فروشنده کد خود را ارائه می‌کند و این کد به صورت خودکار به شماره سپرده‌ی وی نگاشت می‌گردد. سپس تطابق این شماره سپرده با شماره سپرده‌ای که در سند مربوط به رسید دیجیتالی داده شده، بستانکار شده است، چک می‌گردد تا فروشنده مطمئن گردد که رسید دیجیتالی مربوط به وی می‌باشد.

جدول الف-۱ شرح پارامترهای verifyTransaction

مقدار برگشتی تابع: این مقدار در صورتی که مثبت باشد، مبلغ انتقالی (مبلغ کسر شده از کارت مشتری) را نشان می‌دهد و در صورتی که منفی باشد، معرف کد خطاست. شرح کدهای خطا در جدول الف-۳ آمده است.

۲- تابع برگشت تراکنش:

```
double reverseTransaction(
    String RefNum,
    String MID,
    String Username,
    String Password)
```

پارامترهای ورودی تابع

پارامتر	نوع	توضیحات
RefNum	String	رسید دیجیتالی مربوط به تراکنشی که مایل به برگشت آن هستید
MID	String	کد فروشنده

نام کاربری که به صورت پیش فرض برابر MID است	String	Username
کلمه ی عبور	String	Password

در صورت موفقیت، مقدار خروجی این تابع برابر با 1 از نوع double و در صورت عدم موفقیت 1- از نوع double می باشد.

۳- تابع ایجاد و ارسال توکن:

```
string RequestToken (
    string TermID,
    string ResNUM,
    long TotalAmount,
    long SegAmount1,
    long SegAmount2,
    long SegAmount3,
    long SegAmount4,
    long SegAmount5,
    long SegAmount6,
    string AdditionalData1,
    string AdditionalData2,
    long Wage)
```

پارامترهای ورودی تابع

پارامتر	نوع	توضیحات
TermID	string	کد پذیرنده
ResNUM	string	شماره خرید
TotalAmount	long	مبلغ کل تراکنش
SegAmount1	long	به صورت پیش فرض نیازی به ارسال نیست
SegAmount2	long	به صورت پیش فرض نیازی به ارسال نیست
SegAmount3	long	به صورت پیش فرض نیازی به ارسال نیست
SegAmount4	long	به صورت پیش فرض نیازی به ارسال نیست
SegAmount5	long	به صورت پیش فرض نیازی به ارسال نیست
SegAmount6	long	به صورت پیش فرض نیازی به ارسال نیست
AdditionalData1	string	به صورت پیش فرض نیازی به ارسال نیست
AdditionalData2	string	به صورت پیش فرض نیازی به ارسال نیست
Wage	long	مبلغ کارمزد و به صورت پیش فرض نیازی به ارسال نیست

در صورت موفقیت، مقدار خروجی این تابع برابر با توکن ایجاد شده با طول متغیر می باشد.
نمونه توکن ایجاد شده توسط سرور به صورت 71mT5CX0Ds/kZXFojWQ36A می باشد.

توضیحات	کد*
خطای در پردازش اطلاعات ارسالی (مشکل در یکی از ورودی ها و ناموفق بودن فراخوانی متد برگشت تراکنش).	-1
ورودی‌ها حاوی کارکترهای غیرمجاز می‌باشند.	-3
Merchant Authentication Failed (کلمه عبور یا کد فروشنده اشتباه است).	-4
سند قبلا برگشت کامل یافته است.	-6
رسید دیجیتالی تهی است.	-7
طول ورودی‌ها بیشتر از حد مجاز است.	-8
وجود کارکترهای غیرمجاز در مبلغ برگشتی.	-9
رسید دیجیتالی به صورت Base64 نیست (حاوی کاراکترهای غیرمجاز است).	-10
طول ورودی‌ها کمتر از حد مجاز است.	-11
مبلغ برگشتی منفی است.	-12
مبلغ برگشتی برای برگشت جزئی بیش از مبلغ برگشت نخورده‌ی رسید دیجیتالی است.	-13
چنین تراکنشی تعریف نشده است.	-14
مبلغ برگشتی به صورت اعشاری داده شده است.	-15
خطای داخلی سیستم	-16
برگشت زدن جزئی تراکنش مجاز نمی باشد.	-17
IP Address فروشنده نا معتبر است.	-18

جدول الف-۳ شرح کدهای خطا

* مقادیر کدها همگی منفی می باشند.

پ: پارامترهای تبادلی میان سایت فروشنده و سایت پرداخت الکترونیک سامان

پارامترهایی که سایت فروشنده به سایت پرداخت الکترونیک سامان به صورت POST ارائه می‌کند و در ارتباط با اطلاعات تراکنش می‌باشند:

پارامتر	توضیحات
Amount	مبلغ خرید به ریال (عدد صحیح بدون اعشار و پارامتر اضافی)
ResNum	شماره خرید، فاکتور و ... که سمت فروشنده تولید می‌شود.
MID	کد پذیرنده یا فروشنده
RedirectURL	آدرس URL که روی وب سایت فروشنده قرار گرفته است و نتیجه تراکنش به این صفحه به صورت POST ارسال می‌شود.
ResNum1 ResNum2 ResNum3 ResNum4	دیتای اضافی که توسط سایت پذیرنده ارسال و فقط هنگام گزارشگیری در پنل گزارش تراکنش قابل دسترسی می‌باشد.

پارامترهایی که سایت پرداخت الکترونیک سامان به سایت فروشنده به صورت POST برمی‌گرداند:

پارامتر	توضیحات
ResNum	شماره خرید
RefNum	رسید دیجیتالی
State	وضعیت تراکنش
TRACENO	کد رهگیری

نکات:

نکته ۱: در صورتی که پرداخت الکترونیک سامان RefNum تهی به فروشنده برگرداند، به معنای این است که مشکلی در تراکنش توسط خریدار به وجود آمده است.

نکته ۲: در صورتی که تراکنش با موفقیت انجام شده باشد، State برابر با OK خواهد بود (فراموش نشود خروجی تابع verifyTransaction حتما با مبلغ ارسالی اولیه تطبیق داده شود). در غیر این صورت شرح خطای به وجود آمده برگردانده می‌شود. فروشنده به کمک این فیلد می‌تواند دلیل ناموفق بودن تراکنش را به خریدار نشان دهد.

نکته ۳: حتی اگر فروشنده Session Management خود را بر اساس پیاده‌سازی‌های Cookie Based انجام داده باشد، باید ResNum را به پرداخت الکترونیک سامان پاس بدهد چرا که اگر خریدار در سایت پرداخت الکترونیک سامان بیش از حد معمول وقت بگذراند، Session فروشنده در برگشت Expire گردیده است.

نکته ۴: سیستم نسبت به حروف بزرگ و کوچک حساس است و لذا نام متغیرها را به همین ترتیبی که در این مستند ذکر شده است ارسال دارید.

مقادیر فیلد State در پاسخ در جدول زیر آورده شده است، فروشنده موظف است نوع خطای به وجود آمده را با توجه به جدول زیر برای خریدار مشخص کند:

مقدار	مفهوم
Canceled By User	تراکنش توسط خریدار کنسل شده است.
Invalid Amount	مبلغ سند برگشتی، از مبلغ تراکنش اصلی بیشتر است.
Invalid Transaction	درخواست برگشت یک تراکنش رسیده است، در حالی که تراکنش اصلی پیدا نمی شود.
Invalid Card Number	شماره کارت اشتباه است.
No Such Issuer	چنین صادر کننده کارتی وجود ندارد.
Expired Card Pick Up	از تاریخ انقضای کارت گذشته است و کارت دیگر معتبر نیست.
Allowable PIN Tries Exceeded Pick Up	رمز کارت (PIN) ۳ مرتبه اشتباه وارد شده است در نتیجه کارت غیر فعال خواهد شد.
Incorrect PIN	خریدار رمز کارت (PIN) را اشتباه وارد کرده است.
Exceeds Withdrawal Amount Limit	مبلغ بیش از سقف برداشت می باشد.
Transaction Cannot Be Completed	تراکنش Authorize شده است (شماره PIN و PAN درست هستند) ولی امکان سند خوردن وجود ندارد.
Response Received Too Late	تراکنش در شبکه بانکی Timeout خورده است.
Suspected Fraud Pick Up	خریدار یا فیلد CVV2 و یا فیلد ExpDate را اشتباه وارد کرده است (یا اصلا وارد نکرده است).
No Sufficient Funds	موجودی حساب خریدار، کافی نیست.
Issuer Down SIm	سیستم بانک صادر کننده کارت خریدار، در وضعیت عملیاتی نیست.

کلیه خطاهای دیگر بانکی باعث ایجاد چنین خطایی می گردد.	TME Error
---	-----------

نکته

در موقع استفاده از کارت در اینترنت به ۲ شماره رمز نیاز داریم. یکی به نام رایج رمز کارت (PIN) و دیگری کد رمز مجازی (CVV2) می باشد. PIN کارت مورد استفاده در تراکنش های اینترنتی با PIN مورد استفاده در تراکنش های خودپرداز و دستگاه کارتخوان ممکن است متفاوت باشد و در صورت ورود اشتباه ۳ بار و بیشتر باعث غیر فعال شدن کارت می گردد. CVV2 رمزیست که روی کارت و یا پشت کارت چاپ شده و دارای ۳ رقم از ارقام ۱۷ تا ۱۹ شماره کارت است و فقط جهت استفاده از اینترنت بوده و ورود اشتباه آن به سیستم پرداخت باعث غیرفعال شدن کارت نمی گردد. قابل ذکر است برای تعویض PIN کارت باید به ATM بانک مربوطه مراجعه و برای تعویض CVV2 باید به شعبه صادرکننده کارت مراجعه شود.

آدرس سایت پرداخت الکترونیک سامان برای انجام تراکنش و صدور رسید دیجیتالی

ارسال اطلاعات به سایت پرداخت الکترونیک سامان از طریق آدرس ذیل صورت می گیرد:

<https://sep.shaparak.ir/Payment.aspx>

آدرس Web Service Provider

برای فراخواندن Web Method ها باید از یکی از آدرس های ذیل استفاده کنید. برای جزئیات بیشتر، به نمونه کد مربوط به تکنولوژی مورد استفاده خود رجوع کنید:

<https://acquirer.samanepay.com/payments/referencepayment.asmx?WSDL>

<https://acquirer.samanepay.com/payments/referencepayment.asmx>

مشاهده تراکنش های انجام شده بر روی سایت پرداخت الکترونیک سامان

آدرس مشاهده تراکنش های انجام شده:

<https://acquirer.samanepay.com/merchants/>

برای دسترسی به این قسمت باید کد فروشنده و کلمه عبور خود را ارائه کنید.

کد فروشنده شما

برای دریافت آن با بخش پشتیبانی تماس بگیرید.