



نام مستند

راهنمای استفاده از درگاه پرداخت اینترنتی شاپرک

سطح محرمانگی

محرمانه

محل نگهداری

شرکت کارت اعتباری ایران کیش

تعداد صفحات

51

تاریخ آخرین اصلاح

1405/02/26

شماره بازنگری

24



تاریخچه اصلاحات

ردیف	تاریخ	اقدام کننده	توضیحات تغییرات	صفحات
1	1398/10/29	حامدفتحی	ایجاد مستند	
2	1398/11/08	حامدفتحی	اصلاحات نگارشی	
3	1398/11/12	حامدفتحی	اضافه نمودن توضیحاتی در خصوص نحوه تولید پاکت دیجیتال	24
4	1398/11/12	حامدفتحی	اصلاح مثالهای مرتبط با پاکت دیجیتال	25
5	1399/02/20	حامدفتحی	اصلاحاتی در قرارداد خروجی متد استعمال تراکنش	36
6	1399/03/06	حامدفتحی	تغییراتی در قرارداد مرتبط با دریافت نشانه	17
7	1399/06/01	حامدفتحی	امکان دریافت نشانه پرداخت با شرایط ویژه	23
8	1399/06/17	حامدفتحی	افزودن سرویس تراکنش معکوس	35
9	1399/09/04	حامدفتحی	اضافه شدن امکان خرید اعتباری	20
10	1399/10/09	حامدفتحی	اضافه شدن نمودار فعالیت انجام تراکنشهای اینترنتی مبتنی بر توکن	11
12	1400/03/08	آیدا ترکی	جدا شدن متدهای مربوط به دیجی پی در مستند دیجی پی	
13	1400/12/17	احمد ارمان	اضافه شدن امکان پرداخت قبض با تاییدیه	33
15	1401/09/06	خاطره قربانی	اضافه شدن فیلد isbehdadtransaction در سرویس دریافت نشابه ، جدول مشخصات شی request	18
16	1401/09/13	خاطره قربانی	اضافه شدن خطای 936 در جدول کدهای پاسخ / عمل	51
17	1401/10/10	خاطره قربانی	اضافه شدن نکته در مورد استعمال کارت با کد ملی	19
19	1402/03/31	خاطره قربانی	اضافه شدن ستون کد پردازش در جدول transactionType	20
20	1402/03/31	خاطره قربانی	اضافه شدن تصویر درگاه جدید	13
21	1402/03/31	خاطره قربانی	تغییر تصویر رسید پرداخت موفق	33 و 14
22	1402/04/10	خاطره قربانی	تغییر تصویر رسید پرداخت (کد کارتخوان اضافه شده است)	33 و 14



15	اضافه شدن جدول توضیحات پارامترهای رسید پرداخت موفق	خاطره قربانی	1402/04/10	23
51	اضافه شدن خطای 937 در جدول کدهای پاسخ / عمل	خاطره قربانی	1402/07/05	24
19	اضافه شدن فیلد encNationalId (کدملی رمز شده) در سرویس های نشانه گذاری و تاییدیه، بخش مشخصات شی addParam	خاطره قربانی	1402/07/05	25
45	اضافه شدن خطای 17 در جدول کدهای پاسخ / عمل	خاطره قربانی	1403/02/11	26
20	اضافه شدن فیلد IsacoWPP در جدول transactionType و نکته در خرید اعتباری در سرویس دریافت نشانه پرداخت	خاطره قربانی	1403/03/23	27
31	اضافه شدن فیلدهای invoiceId و amount در سرویس ارسال تاییدیه تراکنش پرداخت	خاطره قربانی	1403/09/11	28
32	اصلاح مستند	فناوری	1405/02/26	29



امضا	نام و نام خانوادگی	سمت	
		واحد فناوری	تصویب کننده



فهرست مطالب

1	مقدمه مستند	6
2	نیازمندی ها	6
3	اعتبار سنجی و امنیت	6
4	تعریف واژگان و کلمات	6
5	آدرس پایه نرم افزار پرداخت و سرویس های مرتبط	8
6	فرآیند پرداخت	9
7	نمودار فعالیت انجام تراکنشهای اینترنتی مبتنی بر توکن	10
8	فرایند کاربری از درگاه پرداخت اینترنتی شرکت ایران کیش	11
9	تصویر رسید پرداخت موفق	13
10	نحوه مدیریت تراکنش اصلاحیه (REVERSE) و تاییدیه	28
11	سرویس های نشانه گذاری	15
11.1	سرویس دریافت نشانه پرداخت	15
11.2	هدایت کاربر (دارنده) جهت پرداخت به پرداخت اینترنتی	26
11.3	هدایت کاربر به سایت پذیرنده بعد از پرداخت	27
12.1	سرویس ارسال تاییدیه تراکنش پرداخت	29
12.2	سرویس ارسال تاییدیه تراکنش قبض ویژه	31
13	سرویس تراکنش معکوس	33
12	کدهای پاسخ / عمل	35
13	کوتاه نوشت ها	42



1 مقدمه مستند

مستند حاضر جهت تشریح و توضیح ویژگی ها و نحوه استفاده از خدمت درگاه پرداخت اینترنتی شرکت کارت اعتباری ایران کیش تهیه گردیده است. در این مستند به توضیح فرایند پرداخت در این سامانه و نحوه بهره برداری از سرویس های مرتبط پرداخته می شود.

۲ نیازمندی ها

این سامانه جهت اجرای صحیح و بدون مشکل نیازمند موارد ذیل می باشد:

زبان برنامه نویسی و یا هر ابزاری که توانایی استفاده از web api را داشته باشد.

زبان برنامه نویسی و یا هر ابزاری که توانایی تولید درخواست بر اساس پروتکل HTTP جهت هدایت کاربر به صفحات مرتبط با پرداخت را داشته باشد.

۳ اعتبار سنجی و امنیت

سرویس حاضر برای اعتبارسنجی و اطمینان از صحت اطلاعات دریافتی از پروتکل امن SSL و در برخی از سرویس ها جهت احراز اصالت از مکانیزم پاکت دیجیتال و محدودیت آدرس آی پی استفاده می نماید.

۴ تعریف واژگان و کلمات

M (Mandatory): در این مستند به معنای اجباری بودن مقدار دهی پارامتر ورودی متد می باشد.

O (Optional): در این مستند به معنای اختیاری بودن مقدار دهی پارامتر ورودی متد می باشد.

C (Conditinal): در این مستند به معنای داشتن شرط جهت مقدار دهی پارامتر ورودی متد می باشد.

ابزار پذیرش: عبارت است از سخت افزار یا نرم افزاری که امکان تولید یا شروع یک تراکنش مالی را فراهم می نماید.

پذیرنده: شخصیتی حقیقی یا حقوقی است که میزبان حداقل یک ابزار پذیرش قابل ارائه توسط این شرکت است. به عنوان مثال وبگاهی که فروش کالا یا خدماتی را از طریق درگاه پرداخت اینترنتی این شرکت به انجام می رساند.

دارنده: شخص حقیقی یا حقوقی که به واسطه افتتاح حساب بانکی نزد یکی از بانکها و یا موسسات مالی مجاز، دارای یه کارت بانکی است.

شماره کارت: کدی شامل چهار بخش چهار رقمی، که بر روی کارت بانکی درج شده است.

رمز دوم: عددی شامل 5 تا 12 رقم که توسط دستگاه های خودپرداز بانکهای صادر کننده کارت بانکی با کاربری دارنده کارت ثبت و در تراکنشهای اینترنتی، موبایلی و ... کاربرد دارد.

رمز دوم پویا: عددی شامل 5 تا 12 رقم که توسط نرم افزار و یا سخت افزاری که توسط بانک دارنده در اختیار ایشان قرار گرفته است تولید و به عنوان جایگزین رمز دوم بانکی مورد استفاده قرار می گیرد. رمز دوم پویا همچنین توسط ابزار پذیرش



اینترنتی این شرکت پشتیبانی و در صورت فعال بودن بر روی کارت دارنده و متصل بودن بانک دارنده به سامانه های مرتبط قابل ارائه است.

کد اعتبار سنجی دوم کارت: کدی شامل 3 تا 4 رقم که رو یا پشت کارت بانکی درج می گردد و ممکن است که با عنوان انگلیسی CVV2 مشخص شده باشد. همچنین این کد در صورت نا خوانا یا مخدوش بودن توسط دستگاه خودپرداز بانک صادر کننده کارت بانکی در زمان اختصاص یا تغییر رمز دوم، قابل دریافت می باشد.

تاریخ انقضا: تاریخ انقضا مربوط به سررسید زمان مجاز استفاده از کارت بانکی است و بر روی کارت بانکی درج شده است.

شناسه پرداخت: شامل 1 تا 18 کاراکتر عددی که به منظور شناسایی و رهگیری تراکنش مربوطه در سامانه های بانکی مورد استفاده قرار می گیرد.

تراکنش اصلاحیه (Reverse): به تراکنشی گفته می شود که به منظور عودت وجه به دارنده کارت در صورت بروز اشکال یا شرایط خاص مورد استفاده قرار می گیرد.

کد ارجاع: کدی شامل 12 رقم که به منظور شناسایی تراکنش در سیستم بانکی مورد استفاده قرار می گیرد.

کد پیگیری/اسند: کدی شامل 6 رقم که به منظور شناسایی تراکنش در سیستم بانکی مورد استفاده قرار می گیرد.

شماره پایانه: شناسه ای شامل 8 کاراکتر از حروف 0 تا 9 که معرف پایانه مرتبط با پذیرنده می باشد.

تراکنش تسهیم: به صورت معمول مبالغ کسر شده در زمان انجام تراکنش به یک حساب (که توسط پذیرنده معرفی گردیده است) واریز می گردد. در برخی از کسب کارها لازم است که مبالغ تراکنش بر اساس فرمولی تقسیم و به بیش از یک حساب واریز گردد. به چنین تراکنشی تراکنش تسهیم گفته می شود.

شماره پذیرندگی: شناسه ای شامل 15 کاراکتر از اعداد 0 تا 9 که معرف هویت پذیرنده در سامانه های پرداخت می باشد.

شماره شناسایی بانک: شماره شناسایی بانک (BIN) شامل 6 رقم ابتدایی کارت بانکی است و معرف آن بانک یا موسسه در سیستم بانکداری است. این شناسه یکتا است.

شناسه درخواست: کدی یکتا که می تواند شامل اعداد، حروف و با طول حداکثر 20 کاراکتر باشد، معرف درخواست ارسالی از پذیرنده است و می بایست به ازای تمامی درخواستهای ارسالی از پذیرنده بصورت یکتا تولید گردد.

یکتایی کد تولیدی توسط پذیرنده نزد سامانه های این شرکت بررسی نمی گردد و پذیرنده می بایست با استفاده از الگو یا فرمولی که تضمین کننده یکتایی این کد است استفاده و اقدام به تولید مقادیر نماید.

نشانه (Token): توکن یا نشانه، کدی است (سخت افزار یا نرم افزار) که اجازه انجام فرایندی را در یک سامانه نرم افزاری خارجی فراهم می نماید. نشانه در درگاه پرداخت اینترنتی این شرکت رشته ای است شامل حروف و اعداد و با طولی به اندازه حداکثر 48 کاراکتر که در بازه زمانی 10 دقیقه از زمان تولید معتبر و بعد از اولین پرداخت (با شرایطی) دیگر قابل استفاده نیست.



تراکنش تاییدیه: تراکنش تاییدیه (Verify/Confirm) تاییدی است بر دریافت نتیجه پرداخت توسط پذیرنده و اعلام به سامانه پرداخت جهت واریز وجوه به حساب پذیرنده.

کلمه عبور (Pass Phrase): رشته ای شامل 16 کاراکتر شامل حروف و اعداد که توسط سامانه در زمان اختصاص شناسه پذیرندگی تولید و به همراه بخش عمومی از یک کلید RSA در اختیار پذیرنده قرار می گیرد.

Timestamp: سیستمی است برای تشریح کردن یک نقطه زمانی مشخص که بر اساس گذشت ثانیه ها از یک تاریخ مبدا اندازه گیری میشود. در سامانه های نرم افزاری این شرکت منظور Epoch Time یا POSIX time است که بر اساس ثانیه های گذشته از تاریخ مبدا 1970/01/01 اندازه گیری می گردد. برای دریافت اطلاعات بیشتر می توانید از مراجع زیر استفاده نمایید.

https://en.wikipedia.org/wiki/Unix_time

<https://www.epochconverter.com/>

نوع پارامتر: نوع پارامترهای ورودی و خروجی ذکر شده در جداول، در قسمت کوتاه نوشت های انتهای مستند آورده شده است.

وضعیت ارسال: توضیح وضعیت ارسال ذکر شده برای هر پارامتر در جداول، در قسمت کوتاه نوشت های انتهای مستند آورده شده است.

۵ آدرس پایه نرم افزار پرداخت و سرویس های مرتبط

<https://ikc.shaparak.ir>



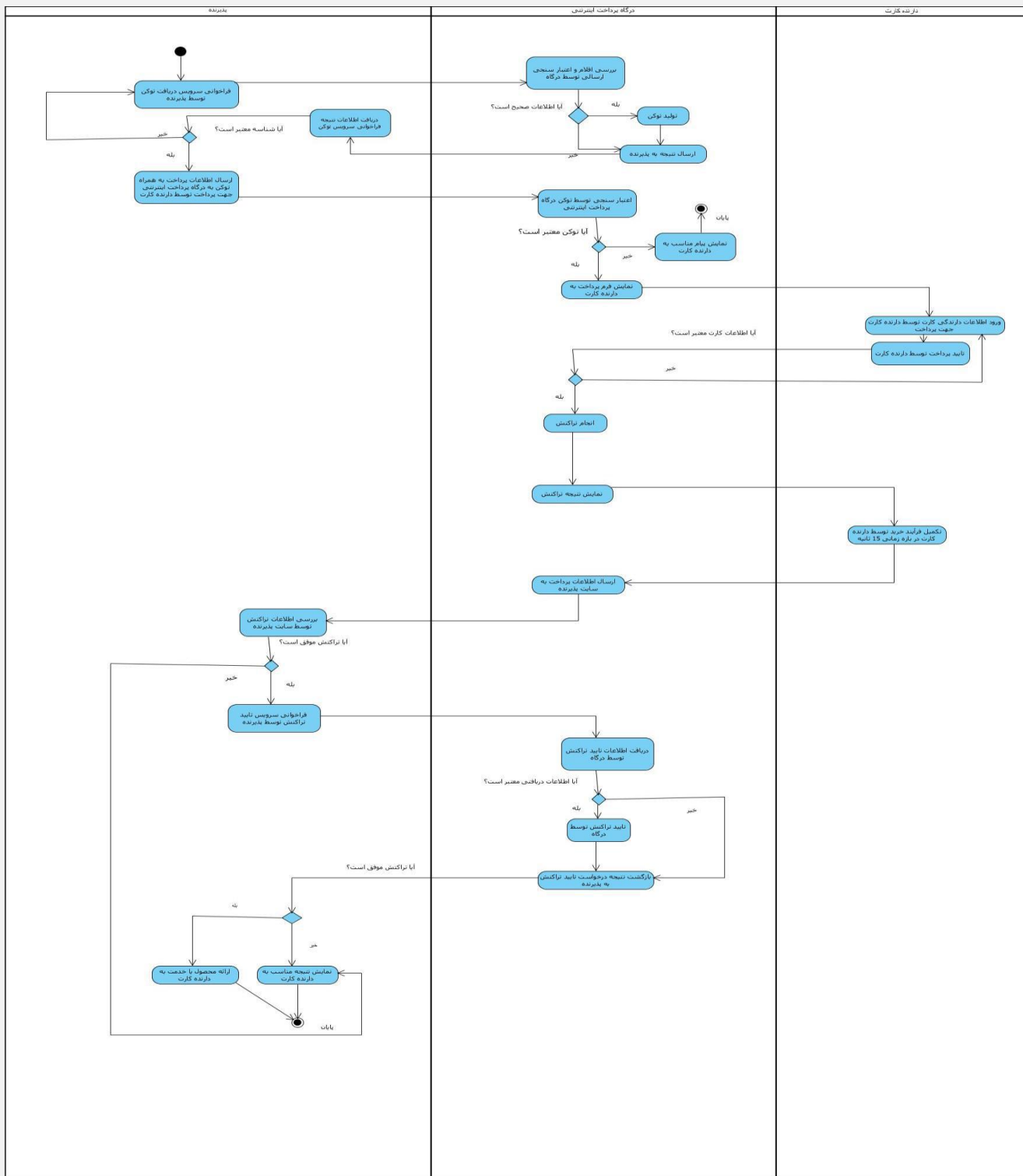
۶ فرآیند پرداخت



1. ارسال درخواست دریافت نشانه به سامانه درگاه پرداخت اینترنتی
2. در صورت دریافت پاسخ موفق از مرحله اول، کاربر از سایت پذیرنده توسط یک درخواست HTTP با متد POST، به نرم افزار پرداخت، هدایت می گردد.
3. نتیجه عملیات پرداخت، توسط نرم افزار پرداخت اینترنتی ایران کیش به آدرس بازگشت ارائه شده توسط پذیرنده، توسط یک درخواست HTTP با متد POST ارسال می گردد.
4. در صورتی که نتیجه عملیات مثبت باشد و سایت پذیرنده قادر به ارائه خدمت باشد، درخواست تاییدیه به سامانه درگاه پرداخت اینترنتی ایران کیش ارسال می گردد.

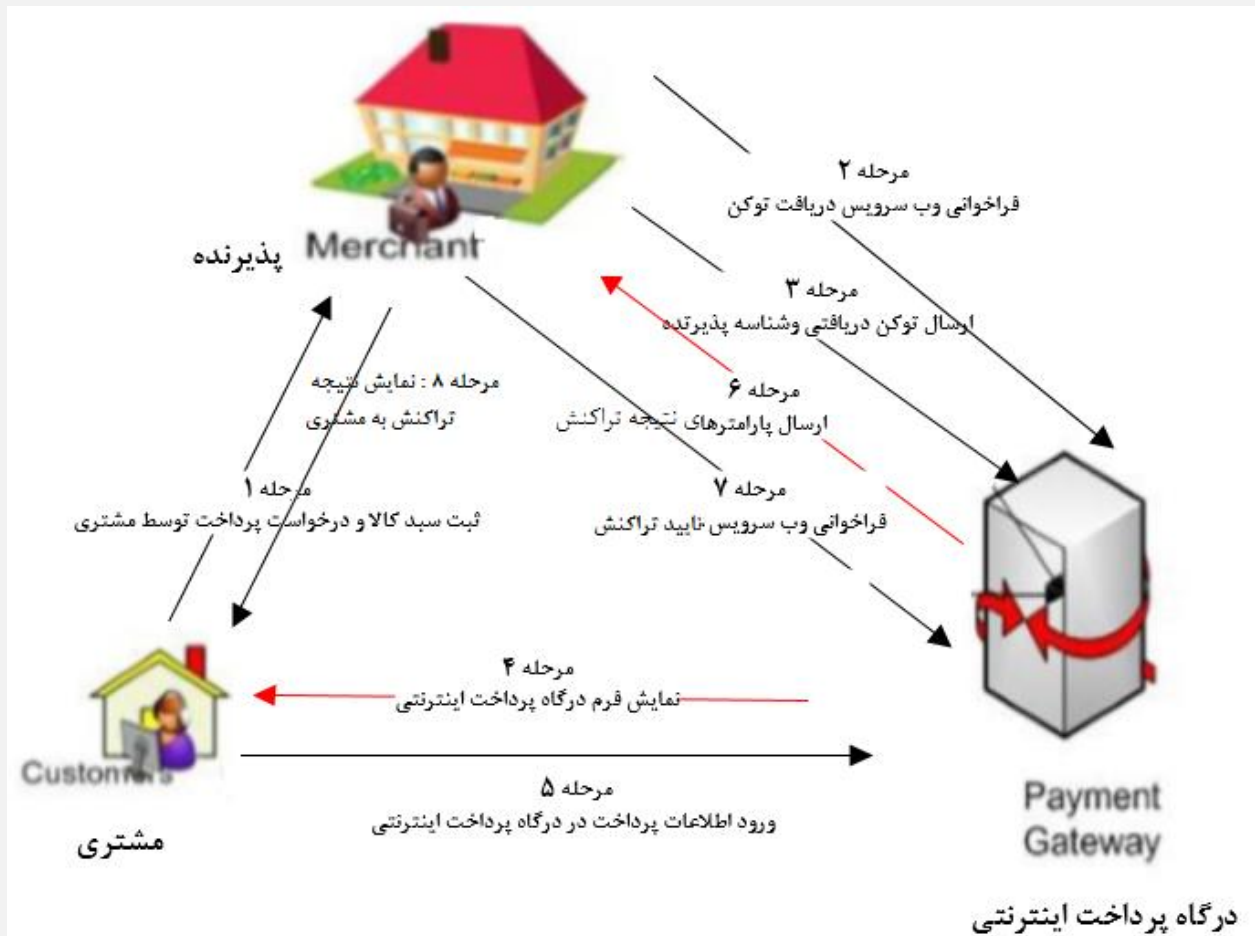


۷ نمودار فعالیت انجام تراکنشهای اینترنتی مبتنی بر توکن





۸ فرایند کاربری از درگاه پرداخت اینترنتی شرکت ایران کیش



مرحله 1: تکمیل سبد خرید و درخواست پرداخت در سایت فروشنده (پذیرنده) توسط خریدار (دارنده کارت)

مرحله 2: فراخوانی وب سرویس درگاه پرداخت اینترنتی توسط سایت پذیرنده و دریافت Token از درگاه پرداخت اینترنتی (MakeSpecialToken , MkeToken). سایت پذیرنده برای دریافت Token ، وب سرویس شرکت ایران کیش را فراخوانی می نماید. خروجی این وب سرویس Token می باشد.



شماره کارت اعتباری
ایران کیش (سهامی عام)

زمان باقیمانده ۰۹:۱۹

شماره کارت

تاریخ انقضا / ماه / سال

CVV۲

کد امنیتی 9 6 2 9 6

رمز پویا دریافت رمز پویا

تلفن همراه (اختیاری)

ایمیل (اختیاری)

ذخیره شماره کارت و تاریخ انقضا

انصراف پرداخت

مبلغ قابل پرداخت ۵۰,۰۰۰ ریال

شرکت خدمات پرداخت کارت اعتباری ایران کیش



آدرس سایت
کد پذیرنده
شماره پایانه

https://ikc.shaparak.ir
۹۹۲۱۸۰۰۰۸۰۹۹۳۶۵
۰۸۰۹۹۳۶۵

اطلاعات پرداخت راهنمای درگاه




۹ تصویر رسید پرداخت موفق

شرکت خدمات پرداخت کارت اعتباری ایران کیش

۰۸۰۹۹۳۶۵	شماره پایانه
۹۹۲۱۸۰۰۰۸۰۹۹۳۶۵	کد پذیرندگی
ikc.shaparak.ir	آدرس سایت
خرید	نوع تراکنش
۵۰,۰۰۰ ریال	مبلغ تراکنش
۰۸:۵۷:۴۹ ۱۴۰۵/۰۲/۲۶	زمان تراکنش
۲۹۴۵۵۴۸۷۰	کد درگاه پرداخت

۶۰۳۷-۹۹##-###-۱۶۵۲	شماره کارت
 بانک ملی ایران	بانک صادر کننده

۰۰۰۰۱۹۹۲۹۵۲۶	شماره مرجع
۱۹۹۲۹۵	شماره پیگیری
۶۲۸۱۵۲۰۷۷	کد رهگیری

پرداخت با موفقیت انجام شد

تکمیل فرایند خرید

۰۰:۳۷ ثانیه تا انتقال به سایت مبدا



جدول توضیحات پارامترهای رسید پرداخت موفق

ردیف	پارامتر	توضیحات
1	نام فروشگاه	از شماره پایانه ای که توسط کاربر وارد میگردد ، بدست می آید
2	شماره پایانه	توسط کاربر در سرویس توکن دریافت میشود
3	کد پذیرندگی	توسط کاربر در سرویس توکن دریافت میشود
4	آدرس سایت	از شماره پایانه ای که توسط کاربر وارد میگردد ، بدست می آید
5	نوع تراکنش	توسط کاربر در سرویس توکن دریافت میشود
6	مبلغ تراکنش	توسط کاربر در سرویس توکن دریافت میشود
7	زمان تراکنش	توسط سرویس پرداخت تولید میگردد
8	کد کارتخوان	توسط سرویس پرداخت تولید میگردد
9	شماره کارت	در زمان پرداخت توسط مشتری پر میگردد
10	بانک صادر کننده	همان بانک صادرکننده کارت مشتری در زمان پرداخت میباشد
11	شماره مرجع	توسط سرویس پرداخت تولید میگردد
12	شماره پیگیری	توسط سرویس پرداخت تولید میگردد
13	کد رهگیری	توسط کاربر در سرویس توکن دریافت میشود

۱۰ سرویس های نشانه گذاری

سرویس های نشانه گذاری بصورت Rest API تولید گردیده است، محتوی ارسالی در پیام های HTTP می بایست به صورت JSON و با سرانه مناسب تولید و در اختیار سامانه های این شرکت قرار گیرد.

10.1 سرویس دریافت نشانه پرداخت

نحوه استفاده از سرویس دریافت نشانه

سرویس دریافت نشانه پرداخت برای احراز هویت از مکانیزم DigitalEnvelope و همچنین محدودیت آی پی آدرس ارسال کننده، استفاده می نماید که در ادامه به توضیحات جزئیات می پردازیم.

مشخصات پیام HTTP

Message Attributes	
Resource	api/v3/tokenization/make
Method	Post
Content Type	application/json
Encoding	UTF-8

مشخصات کلی محتوی پیام درخواست در سرویس دریافت نشانه

Payload (Body) Attributes	
Type	JSON

نام پارامتر	نوع	اجباری/اختیاری	توضیحات
authenticationEnvelope	obj(AuthenticationEnvelope)	M	شامل اطلاعات پاکت دیجیتال
Request	obj(Request)	M	شامل اطلاعات درخواست نشانه

مشخصات شی AuthenticationEnvelope

نام پارامتر	نوع	اجباری/اختیاری	نام فارسی	توضیحات
lv	b	M	بردار تولیدی	در یک الگوریتم رمز نگاری متقارن مورد استفاده قرار می گیرد.
Data	b	M	اطلاعات نتیجه عملیات	نتیجه عملیات رمز نگاری بر اساس مکانیزم پاکت دیجیتال



مشخصات شی Request

نام پارامتر	نوع	اجباری/اختیاری	نام فارسی	توضیحات
transactionType	a	M	نوع تراکنش	مقدار این پارامتر در قسمت در زیر آورده شده است.
terminalId	s(n)8	M	شماره پایانه	
acceptorId	s(n)15	M	شماره پذیرنده	
Amount	n..12	M	مبلغ تراکنش	
revertUri	ans	M	آدرس ارسال پاسخ نتیجه عملیات	
billInfo	obj(BillInfo)	C	اطلاعات قبض پرداختی	
multiplexParameters	array(MultiplexParameter)	C	پارامترهای ترکیبی	شامل اطلاعات مرتبط با خرید تسهیم
requestId	an..20	M	شناسه درخواست	
paymentId	s(n)..18	O	شناسه پرداخت	
cmsPreservationId	ans	O	شناسه مرتبط با مشتری در سامانه های پذیرنده/پرداخت	
requestTimestamp	Epoch time	M	تاریخ و ساعت تولید درخواست در سامانه های پذیرنده	
additionalParameters	array(addParam)	O	آرایه ای از شی addParam	
isbehdadtransaction	b	C	پایانه بهدادی	برای حسابهای بهدادی true میباشد ولی برای غیر بهدادی لازم به ارسال نمیشد.

مشخصات شی addParam

نام پارامتر	نوع	اجباری/اختیاری	نام فارسی	توضیحات
Key	s(n)..32	M	کلید	کلید مرتبط با داده اضافه توافق شده
Value	s(n)..128	M	مقدار	مقدار متناظر با داده اضافه توافق شده



جهت تطابق کد ملی خریدار با پرداخت کننده (دارنده کارت) به شرح زیر مقدار دهی گردد. لازم به توضیح است که این ویژگی به صورت پیش فرض فعال نیست و جهت فعال سازی می بایست به این شرکت درخواست فعالسازی ارائه گردد.

```
{
"Key": "nationalId",
"Value": "0*****844"
}
```

نکته: جهت استعلام کارت با کد ملی، ارسال کد ملی الزامی می باشد و در صورت ارسال نشدن کد ملی، پرداخت با خطا مواجه میگردد.

جهت تطابق کد ملی رمز شده خریدار با پرداخت کننده (دارنده کارت) به شرح زیر مقدار دهی گردد. لازم به توضیح است که این ویژگی به صورت پیش فرض فعال نیست و جهت فعال سازی می بایست به این شرکت درخواست فعالسازی ارائه گردد.

```
{
"Key": "encNationalId",
"Value": "ABCDEADBC65421365445565*****ABCD"
}
```

نکته: جهت استعلام کارت با کد ملی، ارسال کد ملی رمز شده الزامی می باشد و در صورت ارسال نشدن کد ملی رمز شده، دریافت نشانه پرداخت با خطا مواجه میگردد. (این کد توسط سرویس شاپرک نزد مشتری تولید و به شرکت پرداخت ارسال میگردد).

مشخصات شی BillInfo

نام پارامتر	نوع	اجباری/اختیاری	نام فارسی	توضیحات
billId	s(n)..18	M	شناسه قبض	
BillPaymentId	s(n)..18	M	شماره پرداخت قبض	

مشخصات شی MultiplexParameter

نام پارامتر	نوع	اجباری/اختیاری	نام فارسی	توضیحات
iban	an 26	M	شماره شبای واریزی	
amount	n..12	M	مبلغ پرداختی به ازای شماره شبای ارائه شده	



نوع تراکنش (محتوی پارامتر transactionType)

مقدار	نام فارسی	کد پردازش	توضیحات
Purchase	تراکنش خرید	000000	
Bill	تراکنش پرداخت قبض	500000	
SpecialBill	تراکنش قبض با امکان تاییدیه	500000	

پرداخت تسهیمی

جهت انجام یک تراکنش تسهیمی می‌بایست در ابتدا این خدمت توسط سامانه های پرداخت این شرکت برای پذیرنده فعال گردیده باشد، در این صورت پذیرنده در زمان دریافت نشانه باید آرایه ای از شی MultiplexParameter را که شامل شماره شبا و مبلغ است را در پارامتر مرتبط جایگذاری و ارسال نماید. در غیر این صورت تراکنش به صورت یک تراکنش عادی انجام و مبلغ تراکنش به صورت کل با یک حساب تسویه می‌گردد.

پرداخت قبض

جهت انجام یک تراکنش پرداخت قبوض خدماتی، پذیرنده می‌بایست در پارامتر نوع تراکنش مقدار Bill را جایگذاری و شی BillInfo را در پارامتر مرتبط مقداردهی و ارسال نماید.

نحوه تولید پاکت دیجیتال

یک پاکت دیجیتالی یک محفظه الکترونیکی ایمن است که برای محافظت از پیام از طریق رمزنگاری و تأیید صحت داده ها استفاده می‌نماید.

یک پاکت دیجیتال از دو لایه برای رمزگذاری استفاده می‌کند، رمزنگاری بر اساس یک الگوریتم متقارن و رمزنگاری بر اساس یک الگوریتم نامتقارن و بر پایه کلید عمومی.

از الگوریتم متقارن برای رمزنگاری و رمزگشایی پیام و از الگوریتم نامتقارن برای ارسال کلید مخفی مرتبط با الگوریتم متقارن از طریق شبکه استفاده می‌شود.

بعد از دریافت پاکت دیجیتال نزد سامانه های پرداخت، با استفاده از کلید خصوصی مرتبط با پذیرنده ابتدا محتوی پارامتر data رمزگشایی و سپس با در اختیار گرفتن کلید مخفی الگوریتم متقارن و بردار ارسالی، عملیات رمزگشایی اطلاعات ارسالی انجام می‌پذیرند.



در این سامانه از الگوریتم متقارن AES و الگوریتم نامتقارن RSA برای این منظور به‌گیری شده است.

مشخصات مورد انتظار در رمز نگاری AES

Cipher Mode : CBC

Padding = PKCS7

Key Size : 128

مراحل انجام کار:

1. تولید یک رشته از اطلاعات ارسالی در درخواست نشانه به توضیحات زیر:

- در صورتی که هدف یک پرداخت عادی و یا پرداخت قبض باشد :

“00” + مبلغ کل تراکنش ، گسترش پیدا کرده با صفر از سمت چپ تا 12 رقم + کلمه عبور + شماره پایانه

به عنوان مثال : پرداختی با مبلغ 1000 ریال و با شماره پایانه 02000001 و با کلمه عبور AAFF124578127138 را در نظر بگیرید، نتیجه تولید رشته پایه به توضیحات زیر خواهد بود:

```
var bStr=02000001AAFF12457812713800000000100000
```

- در صورت پرداخت تسهیم

می‌بایست تمامی شباهای شرکت کننده در پرداخت به همراه مبالغ مرتبط در رشته شرکت کنند.

همچنین می‌بایست حروف IR که در ابتدای رشته شماره شبا قرار می‌گیرند با معادل عددی 2718 طبق استاندارد مرتبط جایگزین و در رشته قرار گیرد.

مبلغ واریزی به + شماره شبا اول + “01” + مبلغ کل تراکنش ، گسترش پیدا کرده با صفر از سمت چپ + کلمه عبور + شماره پایانه
مبلغ واریزی به شبای دوم، گسترش پیدا کرده با صفر از + شماره شبا دوم + شبای اول، گسترش پیدا کرده با صفر از سمت چپ تا 12 رقم
+ مبلغ واریزی به شبای ...، گسترش پیدا کرده با صفر از سمت چپ تا 12 رقم + شماره شبا ... + سمت چپ تا 12 رقم

به عنوان مثال : پرداخت دو تسهیمی با مبلغ کل 1000 ریال و با شماره پایانه 02000001 و با کلمه عبور AAFF124578127138 را در نظر بگیرید:

```
{
  "iban": "IR870180000000008322908440,"
  "amount":450},// مبلغ واریزی به شبای اول
{
  "iban": "IR680120010000003187611452,"
  "amount":550// مبلغ واریزی به شبای دوم
}}
```



ابتدا حروف IR که در ابتدای رشته شماره شبا قرار دارد را با عدد 2718 جایگزین می‌کنیم:

```

{{
  "iban": "2718870180000000008322908440,"
  "amount":450},// مبلغ واریزی به شبای اول
  {
  "iban": "2718680120010000003187611452,"
  "amount":550// مبلغ واریزی به شبای دوم
  }}
    
```

سپس با چسباندن مقادیر آمده در شیوه ساخت رشته که قبلا توضیح داده شد، به رشته زیر خواهیم رسید :

```

var bStr =
02000001127138AAFF124578000000001000012718870180000000008322908440000000004502718
680120010000003187611452000000000550
    
```

2. سپس رشته تولید شده در مرحله اول را به عنوان رشته ای از کد HEX در نظر گرفته و آن را به یک آرایه از بایت تبدیل می‌کنیم.
 3. بر اساس الگوریتم متقارن AES یک کلید و بردار به طول 128 بیت تولید می‌نماییم .
 4. آرایه حاصل از نتیجه مرحله دوم را با استفاده از کلید و بردار مرحله سوم رمز می‌نماییم .
 5. از آرایه حاصل در نتیجه مرحله چهارم بر اساس الگوریتم SHA256 ، HASH محاسبه می‌نماییم.
 6. آرایه ای از بایت ها به طول 48 بایت تولید و در 16 بایت اول ، کلید تولیدی در مرحله سوم و در 32 بایت انتهایی، آرایه حاصل از نتیجه مرحله پنجم را قرار می‌دهیم.
 7. آرایه حاصل در مرحله ششم را با استفاده از کلید عمومی ارائه شده توسط سامانه بر اساس الگوریتم RSA رمز و به صورت یک رشته از کد HEX در پارامتر data از شی AuthenticationEnvelope جایگذاری می‌نماییم .همچنین بردار تولیدی در مرحله سوم را به صورت یک رشته از کد HEX در پارامتر iv جایگذاری می‌نماییم.
- مثال :پرداخت تسهیمی با شرایط زیر را در نظر بگیرید:

```

AES Secret Key : E29F6D7A52373DD4398B76EFA690055E (HEX Presentation)
AES Initializing Vector : 8F5C757DAFA895501B5F9E8F286C64CC (HEX Presentation)
Pass Phrase : 127138AAFF124578
Public Key : (PEM)
-----BEGIN PUBLIC KEY-----
MIGfMA0GCsqGSIb3DQEBQUAA4GNADCBiQKBgQDYnwnVWP5SYVlaUrHShDKYbK7R
sB0c+52k0KZdJRKMtt09ILNw3xPmcZMV5lhWr3//qJQBPR+O8TF0szPG9+LkUX5h
uWgP8aMAvEcMNzWZ7gP9O0PHB8HrcV/3Y1nlfYjtpawspcUvdhM4Q1ps4JXLha5v
BaxOM2hGLXGHo2o5rQIDAQAB
    
```



-----END PUBLIC KEY-----

Request :

```
"request": {
  "acceptorId": "992*****523",
  "amount": 1000,
  "billInfo": null,
  "cmsPreservationId": "98912*****",
  "multiplexParameters": [
    {
      "amount": 550,
      "iban": "IR870180000000008322908440"
    },
    {
      "amount": 450,
      "iban": "IR680120010000003187611452"
    }
  ],
  "paymentId": null,
  "requestId": "8eb9f6f829c4914 ",
  "requestTimestamp": 1576681231,
  "revertUri": "http://www.irankish.com/...",
  "terminalId": "02010523",
  "transactionType": "Purchase"
}
```



رشته پایه به توضیحات زیر خواهد بود (مرحله اول):

02010523127138AAFF1245780000000010000127188701800000000083229084400000000055027186801200100000031876114520000000004
50

نتیجه رمز نگاری با الگوریتم AES و کلید و بردار ارائه شده به توضیحات زیر است (مرحله چهارم):

(HEX Presentation)

3E236B55D2AE35B100B1243BF6436F082B0B246AECC86D4B305FBEA9A72E74133647513C6C7DD71F
F0E37B9B1A0E9511D0B3952B065B46598ADF5535A0C78EF9

نتیجه محاسبه HASH بر اساس SHA256 به توضیحات زیر است (مرحله پنجم):

(HEX Presentation)

E43F841F3FCF3CD0F2B15E2D2F399E2118F628F3C4F35DDB35AA2BF917BB2FC0

نتیجه تولید آرایه شامل کلید و HASH به توضیحات زیر است (مرحله ششم):

(HEX Presentation)

E29F6D7A52373DD4398B76EFA690055E43F841F3FCF3CD0F2B15E2D2F399E2118F628F3C4F35DDB35AA2BF917BB2FC0

نتیجه رمز نگاری بر اساس الگوریتم RSA و کلید عمومی به توضیحات زیر است (مرحله هفتم):

(HEX Presentation)

9785A9F9A91D6A303C7E0BF47E1E659F1F0DFBECB948D606239F64F4501207E93E86609CC35EFCEBA
5FDF8459AF290373816EA25E4CEB75FB7D53B9729C167873A74C55CD7DC1844A2A37AD06641C65F4
2D845D77D09DE9B382F91F6CFDD38CBC7306ACD0C7815693F916809007459B27510BFF93CA98
2AC5B2F6BFCFB641DD0



در نهایت JSON تولیدی برای درخواست نشانه به توضیحات زیر خواهد بود:

```
{
  "authenticationEnvelope": {
    "data":
    "9785A9F9A91D6A303C7E0BF47E1E659F1F0DFBECB948D606239F64F4501207E93E86609CC35EFCEBA
    5FDF8459AF290373816EA25E4CEB75FB7D53B9729C167873A74C55CD7DC1844A2A37AD06641C65F4
    2D845D77D09DE9B382F91F6CFDD38CBC7306ACD0C7815693F916809007459B27510BFF93CA982AC5
    B2F6BFCFB641DD0
    ",
    "iv": "8F5C757DAFA895501B5F9E8F286C64CC"
  },
  "request": {
    "acceptorId": "992*****523",
    "amount": 1000,
    "billInfo": null,
    "cmsPreservationId": "98912*****",
    "multiplexParameters": [
      {
        "amount": 550,
        "iban": "IR870180000000008322908440"
      },
      {
        "amount": 450,
        "iban": "IR680120010000003187611452"
      }
    ],
    "paymentId": null,
    "requestId": "8eb9f6f829c4914 ",
    "requestTimestamp": 1576681231,
    "revertUri": "http://www.irankish.com/...",
    "terminalId": "02010523",
    "transactionType": "Purchase"
  }
}
```



خروجی سرویس دریافت نشانه برای مثال فوق به صورت زیر خواهد بود:

```
{
  "description": null,
  "responseCode": "00",
  "result": {
    "billInfo": {
      "billId": null,
      "billPaymentId": null
    },
    "expiryTimestamp": 1579449098,
    "initiateTimestamp": 1579448498,
    "token": "981AFD2D2830D3478F357B9CABC8B82D0523",
    "transactionType": "Purchase"
  },
  "status": true
}
```



نحوه استفاده از ویژگی ذخیره و نمایش اطلاعات کارتهای دارنده

سامانه پرداخت اینترنتی این شرکت، امکان ذخیره کارتهای دارنده بر اساس شناسه ای از Profile کاری دارنده که حتما مشتری وبگاه پذیرنده است را فراهم، و در صورتی که کارت یا کارتهایی برای دارنده نزد این سامانه ذخیره شده باشد در دفعات آتی جهت سهولت در پرداخت، لیست و تاریخ انقضای کارتها در سامانه برای ایشان در دسترس خواهد بود.

بدلیل عدم امکان استفاده از کوکی و مکانیزم های مشابه (قوانین امنیتی، بالادستی و فنی) در سامانه درگاه پرداخت اینترنتی این ویژگی کاملا وابسته به شناسه ارسالی از وبگاه پذیرنده است.

بدلیل گسترش پرداخت بدون حضور کارت در فضای اینترنت و نرم افزارهای تلفن همراه پیشنهاد می گردد که این شناسه با توجه به Profile کاری دارنده نزد وبگاه پذیرنده، شماره موبایل ایشان انتخاب و ارسال گردد. در حال حاضر این سامانه از شماره تلفن همراه و آدرس پست الکترونیک برای ارائه این خدمت پشتیبانی می نماید.

جهت بهره گیری از این ویژگی کفایست شماره موبایل و یا آدرس پست الکترونیک دارنده در سرویس دریافت نشانه در پارامتر cmsPreservationId ارائه گردد.

در صورت ارائه شماره تلفن همراه به عنوان شناسه می بایست حتما از الگوی زیر تبعیت گردد، همچنین در صورت ارائه آدرس پست الکترونیک، می بایست آدرس حتما از الگوی صحیح برخوردار باشد.

Mobile : "^989[0-9]{2}[0-9]{7}\$"

Mail Address : ^(?(")(".+?(?!\\)"@)|((([0-9a-z](\.(?!\.)|[-!#\\$\%&'*\+\/=?\^\`{\}|\~\w))*)(?<=[0-9a-z])@))?(\\)(\[[d{1,3}\.]{3}\d{1,3}\])|((([0-9a-z](-\w)*[0-9a-z]*\.)+[a-z0-9](-a-z0-9){0,2}[a-z0-9]))))\$

به عنوان مثال : شناسه های زیر در این سامانه معتبر می باشد.

98912124***6

someone@somewhere.something

به عنوان مثال : شناسه های زیر در این سامانه معتبر نمی باشد.

0912124***6

912124***6

+98912124***6

someone.somewhere.something

blablabla.com

در صورتی که محتوی این پارامتر از الگوی اعلامی تبعیت ننماید، خطایی در ارائه نشانه رخ نداده و صرفا این ویژگی در زمان پرداخت قابل استفاده نمی باشد.



10.2 هدایت کاربر (دارنده) جهت پرداخت به پرداخت اینترنتی

بعد از دریافت نشانه پرداخت که قبلا در این مستند توضیح داده شده است، جهت انجام عملیات مرتبط می بایست کاربر توسط تولید یک درخواست HTTP با متد POST به صفحه درگاه پرداخت اینترنتی این شرکت منتقل گردد.

مشخصات پیام HTTP

Message Attributes	
Resource	/iui3/IPG/Index/
Method	Post
Content Type	application/x-www-form-urlencoded
Enctype	multipart/form-data
Encoding	UTF-8



مشخصات کلی محتوی پیام هدایت کاربر به نرم افزار پرداخت

نام پارامتر	نوع	اجباری/اختیاری	نام فارسی	توضیحات
tokenId	an..48	M	شناسه نشانه	




11.3 هدایت کاربر به سایت پذیرنده بعد از پرداخت

پس از وارد کردن پارامترهای ورودی جهت پرداخت و انجام عملیات پرداخت، صفحه "صدور رسید خرید" به صورت زیر جهت نمایش اطلاعات تراکنش خرید، نمایش داده می شود:

شرکت خدمات پرداخت کارت اعتباری ایران کیش

۰۸۰۹۹۳۶۵	شماره پایانه
۹۹۲۱۸۰۰۰۸۰۹۹۳۶۵	کد پذیرندگی
ikc.shaparak.ir	آدرس سایت
خرید	نوع تراکنش
۵۰,۰۰۰ ریال	مبلغ تراکنش
۰۸:۵۷:۴۹ ۱۴۰۵/۰۲/۲۶	زمان تراکنش
۲۹۴۵۵۴۸۷۰	کد درگاه پرداخت

۶۰۳۷-۹۹##-###-۱۶۵۲	شماره کارت
 بانک ملی ایران	بانک صادر کننده

۰۰۰۰۱۹۹۲۹۵۲۶	شماره مرجع
۱۹۹۲۹۵	شماره پیگیری
۶۲۸۱۵۲۰۷۷	کد رهگیری

پرداخت با موفقیت انجام شد	
<div style="background-color: #006666; color: white; padding: 5px; display: inline-block; border-radius: 5px;">تکمیل فرایند خرید</div>	
<small>۰۰:۳۷ ثانیه تا انتقال به سایت مبدا</small>	



با زدن دکمه "تکمیل خرید وانتقال به سایت پذیرنده"، تراکنش پرداخت تکمیل شده و کاربر به سایت پذیرنده هدایت می شود و اطلاعات پرداخت برای پذیرنده ارسال می شود این اطلاعات به شرح جدول ذیل می باشد

مشخصات کلی محتوی پیام پاسخ پرداخت به آدرس برگشت وبگاه پذیرنده

نام پارامتر	نوع	وضعیت ارسال	نام فارسی	توضیحات
token	an..48	Y	شناسه نشانه	
acceptorId	s(n) 15	Y	شماره پذیرنده	
responseCode	an 2	Y	کد نتیجه عملیات	
paymentId	s(n) ..18	C	شناسه پرداخت	
RequestId	an..20	Y	شناسه درخواست	
sha256OfPan	b	C	HASH شماره کارت بر اساس SHA256	
retrievalReferenceNumber	s(n) 12	C	شماره ارجاع	
amount	s(n) ..12	Y	مبلغ تراکنش	
maskedPan	s(n) 16	C	شماره کارت به صورت ماسک شده	
systemTraceAuditNumber	s(n) ..6	C	شماره سند/پیگیری	

پذیرنده با مشاهده اطلاعات پرداخت در صورت پرداخت موفق اقدام به ارسال سرویس استعلام و تاییدیه برای پرداخت مورد نظر می کند ، در صورت دریافت نتیجه موفق سرویس تاییدیه اقدام به تحویل کالا به دارنده کارت می کند

12 نحوه مدیریت تراکنش تاییدیه و اصلاحیه (Reverse)

تراکنش تاییدیه معادل تراکنش با شاخص 0220 در سامانه های پرداخت بر اساس استاندارد ISO8583 است، این تراکنش به منظور اطمینان از دریافت نتیجه پرداخت توسط پذیرنده و ارسال درخواست تسویه پیش بینی گردیده است.

این تراکنش در درگاه پرداخت اینترنتی این شرکت حداکثر 20 دقیقه از زمان پرداخت (تراکنش شاخص 0200 در استاندارد ISO) معتبر می باشد و پس از این زمان به این درخواست ترتیب اثر داده نخواهد شد.

تراکنش اصلاحیه (Reverse) جهت عودت وجه برداشتی از حساب دارنده پیش بینی و در شرایط خاص جهت عودت مبلغ مورد استفاده قرار می گیرد.



تراکنش اصلاحیه (Reverse) در سامانه در گاه پرداخت اینترنتی ایران کیش به صورت خودکار پیاده سازی گردیده و کنترل اجرا یا عدم اجرای این تراکنش در اختیار پذیرنده نیست. لذا در صورتی که سامانه های این شرکت تراکنش تاییدیه را در بازه زمانی 20 دقیقه از انجام عملیات پرداخت دریافت نمایند به صورت خودکار مبلغ برداشتی از حساب دارنده را عودت و به حساب ایشان بر می گرداند.

پذیرنده موظف است در صورت دریافت پاسخ موفق از نتیجه فرایند پرداخت و بعد از طی مراحل کسب کاری سامانه های داخلی خویش در صورت رسیدن به نتیجه صحیح در بازه زمانی مقرر نسبت به ارسال تراکنش تاییدیه اقدام نماید، در غیر این صورت مبلغ کسر شده به حساب دارنده عودت و تراکنش ناموفق اعلام می گردد.

عواقب احتمالی در خصوص عدم ارسال به موقع تراکنش تاییدیه مستقیماً متوجه پذیرنده می باشد و این شرکت مسئولیتی در این حوزه نمی پذیرد.

در صورتی که پذیرنده در پاسخ سرویس ارسال تراکنش تاییدیه کد 00 و نتیجه موفق دریافت نماید مبلغ تراکنش حتماً به حساب ایشان واریز خواهد گردید.

در مواردی نادر ممکن است علی رقم ارسال تراکنش تاییدیه، به دلیل ویژگی ها و شرایط سامانه های پرداخت تراکنش با تاخیر 72 ساعته به حساب پذیرنده واریز گردد. به این دسته از تراکنشها تراکنش RA گفته می شود که اغلب در زمان Cutoff اتفاق می افتد و با تاخیر 72 ساعته تسویه می گردند.

12.1 سرویس ارسال تاییدیه تراکنش پرداخت

هدف از ارائه این سرویس و ساز و کار مرتبط قبلاً در این مستند توضیح داده شده است.

لازم به توضیح است که در تراکنش پرداخت قبض ارسال تراکنش تاییدیه مجاز نیست و نیاز به ارسال این تراکنش هم نمی باشد.

مشخصات پیام HTTP

Message Attributes	
Resource	api/v3/confirmation/purchase
Method	Post
Content Type	application/json
Encoding	UTF-8

مشخصات کلی محتوی پیام ارسال تاییدیه

Payload (Body) Attributes	
Type	JSON

مشخصات محتوی درخواست سرویس ارسال تاییدیه

نام پارامتر	نوع	اجباری/اختیاری	نام فارسی	توضیحات
terminalId	s(n) 8	M	شماره پایانه	
retrievalReferenceNumber	s(n) 12	M	شماره ارجاع	
systemTraceAuditNumber	s(n) 6	M	شماره سند/پیگیری	
tokenId	an..48	M	شناسه نشانه	
invoiceId	an..20	O	شناسه درخواست	
amount	s(n) ..12	O	مبلغ تراکنش	

نکته: فیلد invoiceId معادل فیلد requestId در سرویس دریافت نشانه پرداخت می باشد.

مشخصات کلی محتوی پیام پاسخ در سرویس ارسال تاییدیه

نام پارامتر	نوع	وضعیت ارسال	نام فارسی	توضیحات
responseCode	an 2	Y	کد نتیجه عملیات	
description	an	Y	توضیحات مرتبط با عملیات	
status	Bool	Y	نتیجه کلی عملیات	
result	obj(TransactionResponse)	C	نتیجه	در صورتی که نتیجه کلی عملیات موفق باشد، result شامل اطلاعات مرتبط با نشانه خواهد بود.



مشخصات شی TransactionResponse

نام پارامتر	نوع	وضعیت ارسال	نام فارسی	توضیحات
responseCode	an 2	Y	نتیجه عملیات تاییدیه	
systemTraceAuditNumber	s(n) 6	C	شماره سند/پیگیری	
retrievalReferenceNumber	s(n) 12	C	شماره ارجاع	
transactionDate	n ..8	Y	تاریخ انجام تراکنش	
transactionTime	n ..6	Y	ساعت انجام تراکنش	
processCode	s(n) 6	C	کد نوع عملیات	
billType	s(n) ..18	C	شناسه قبض	
billId	s(n) ..18	C	شناسه پرداخت قبض	
paymentId	s(n) ..18	C	شناسه پرداخت	
amount	s(n) ..12	Y	مبلغ تراکنش	

12.2 سرویس ارسال تاییدیه تراکنش قبض ویژه

هدف از ارائه این سرویس، همچنین ساز و کار مرتبط قبلا در این مستند توضیح داده شده است. لازم به توضیح است که در تراکنش پرداخت قبض، ارسال تراکنش تاییدیه مجاز نیست و فقط در صورتی که تراکنش قبض و توکن تراکنش از نوع ویژه باشد نیاز به ارسال این تراکنش می‌باشد. مشخصات پیام HTTP

Message Attributes	
Resource	api/v3/confirmation/bill
Method	Post
Content Type	application/json
Encoding	UTF-8

مشخصات کلی محتوی درخواست تاییدیه

Payload (Body) Attributes	
Type	JSON

نام پارامتر	نوع	اجباری/اختیاری	نام فارسی	توضیحات
terminalId	s(n) 8	M	شماره پایانه	
retrievalReferenceNumber	s(n) 12	M	شماره ارجاع	
systemTraceAuditNumber	s(n) 6	M	شماره سند/پیگیری	
tokenId	an..48	M	شناسه نشانه	

مشخصات کلی محتوی پاسخ سرویس تاییدیه

نام پارامتر	نوع	وضعیت ارسال	نام فارسی	توضیحات
responseCode	an 2	Y	کد نتیجه عملیات	
description	an	Y	توضیحات مرتبط با عملیات	
status	Bool	Y	نتیجه کلی عملیات	
result	obj(TransactionResponse)	C	نتیجه	در صورتی که نتیجه کلی عملیات موفق باشد، result شامل اطلاعات مرتبط با نشانه خواهد بود.

مشخصات شی TransactionResponse

نام پارامتر	نوع	وضعیت ارسال	نام فارسی	توضیحات
responseCode	an 2	Y	نتیجه عملیات تاییدیه	
systemTraceAuditNumber	s(n) 6	C	شماره سند/پیگیری	
retrievalReferenceNumber	s(n) 12	C	شماره ارجاع	
transactionDate	n ..8	Y	تاریخ انجام تراکنش	
transactionTime	n ..6	Y	ساعت انجام تراکنش	
processCode	s(n) 6	C	کد نوع عملیات	
billType	s(n) ..18	C	شناسه قبض	
billId	s(n) ..18	C	شناسه پرداخت قبض	
paymentId	s(n) ..18	C	شناسه پرداخت	
amount	s(n) ..12	Y	مبلغ تراکنش	



12.3. سرویس تراکنش اصلاحیه

هدف از ارائه این سرویس ، ارایه امکان عودت مبلغ تراکنش به دارنده ی کارت (ReverseTransaction) در بازه ی زمانی مشخص شده و مورد نیاز پذیرنده می باشد. با استفاده از این ویژگی ، پذیرنده می تواند در صورتی که تراکنش اصلی را با استفاده از متد " ارسال تاییدیه تراکنش " تایید کرده باشد، نسبت به لغو آن و بازگشت مبلغ تراکنش به دارنده ی کارت اقدام نماید.

نکته : امکان لغو تراکنش صرفا تا قبل از ساعت 23:45 منهای مدت زمان تعیین شده همان روز می باشد . برای مثال در صورتی که مدت زمان تعیین شده توسط پذیرنده 45 دقیقه باشد طبیعتا امکان لغو تراکنش بعد از ساعت 23 همان روز وجود نخواهد داشت.

نکته : برای استفاده از این ویژگی پذیرنده باید طی مکاتبه رسمی درخواست خود را به شرکت ایران کیش اعلام نماید.

مشخصات پیام HTTP

Message Attributes	
Resource	api/v3/confirmation/reversePurchase
Method	Post
Content Type	application/json
Encoding	UTF-8

مشخصات کلی محتوی درخواست تراکنش معکوس

نام پارامتر	نوع	اجباری/اختیاری	نام فارسی	توضیحات
terminalId	s(n) 8	M	شماره پایانه	
retrievalReferenceNumber	s(n) 12	M	شماره ارجاع	
systemTraceAuditNumber	s(n) 6	M	شماره سند/پیگیری	
tokenId	an..48	M	شناسه نشانه	



مشخصات کلی محتوی پاسخ در سرویس تراکنش معکوس

نام پارامتر	نوع	وضعیت ارسال	نام فارسی	توضیحات
responseCode	an 2	Y	کد نتیجه عملیات	
description	an	Y	توضیحات مرتبط با عملیات	
status	Bool	Y	نتیجه کلی عملیات	
result	obj(TransactionResponse)	C	نتیجه	در صورتی که نتیجه کلی عملیات موفق باشد، result شامل اطلاعات مرتبط با نشانه خواهد بود.

مشخصات شی TransactionResponse

نام پارامتر	نوع	وضعیت ارسال	نام فارسی	توضیحات
responseCode	an 2	Y	نتیجه عملیات عودت	
systemTraceAuditNumber	s(n) 6	C	شماره سند/پیگیری	
retrievalReferenceNumber	s(n) 12	C	شماره ارجاع	
transactionDate	n ..8	Y	تاریخ انجام تراکنش	
transactionTime	n ..6	Y	ساعت انجام تراکنش	
processCode	s(n) 6	C	کد نوع عملیات	
billType	s(n) ..18	C	شناسه قبض	
billId	s(n) ..18	C	شناسه پرداخت قبض	
paymentId	s(n) ..18	C	شناسه پرداخت	
amount	s(n) ..12	Y	مبلغ تراکنش	



۱۱ کدهای پاسخ / عمل

کدهای پاسخ مرتبط با تراکنش در این سامانه بر اساس استاندارد ISO8583 است، در زیر برخی از کدهای پرکاربرد در این مستند آورده شده است برای مشاهده تمامی پاسخ های مرتبط با این استاندارد می توانید به آدرس زیر مراجعه نمایید.

https://en.wikipedia.org/wiki/ISO_8583#Response_code

همچنین لازم به توضیح است که کدهای سه رقمی که با عدد 9 شروع می گردد مرتبط به این استاندارد نیست و با ساز و کارهای داخلی این سامانه مرتبط است.

کد خطا	شرح خطا	علت خطا	نحوه رفع مشکل
3	پذیرنده فروشگاه نا معتبر است	اطلاعات پذیرندگی در سوئیچ شاپرک غیر فعال می باشد.	از طریق سامانه تیکتینگ به منظور رفع مشکل به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) ارجاع می شود.
5	از انجام تراکنش صرف نظر شد / DO NOT HONOUR / صف پر شده است	کارت معتبر نیست	می بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.
12	خطای 12/ تراکنش نامعتبر	عدم انجام تراکنش با برخی از کارت های بانکی به دلیل غیرفعال بودن گزینه خرید بر روی کارت	می بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.
13	خطای 13/ مبلغ نامعتبر	تعیین سقف مبلغ خرید بر روی کارت	می بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.
17	خطای 17 / کنسل شدن خرید توسط کاربر		
64	مبلغ تراکنش نادرست است، جمع مبالغ تقسیم وجوه برابر مبلغ کل تراکنش نمی باشد		
94	تراکنش تکراری است		مشکل مقطعی، سعی مجدد در زمان دیگر
		مشخص نبودن وضعیت تراکنش	مشکل مقطعی، سعی مجدد در زمان دیگر
5-2	تراکنش اصلی یافت نشد	اشکال در سوئیچ خدمات	در صورت تماس پذیرنده و اعلام عدم رفع مشکل بعد از 24 ساعت کاری، با ذکر توضیحات و ثبت شماره موبایل شخص تماس گیرنده در قسمت توضیحات از طریق سامانه تیکتینگ به منظور رفع مشکل به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) ارجاع می شود.
77	روز مالی تراکنش نا معتبر است	تراکنش در زمان Cut Off انجام شده است	مبلغ بعد از 96 ساعت به حساب دارنده درگاه واریز می شود.



در صورت عدم واریز طی 96 ساعت، به واحد مغایرت از طریق ثبت در پورتال مغایرت ارسال می‌شود.	تراکنش در زمان Cut Off انجام شده است		
		کد تولید کد اعتبار سنجی نامعتبر است	97
مشکل مقطعی، سعی مجدد در زمان دیگر		فرمت پیام نادرست است	30
سیستمی (در صورت کسر مبلغ، تا 72 ساعت کاری مبلغ به حساب دارنده کارت عودت داده می‌شود).	مغایرت سیستمی	تراکنش مالی تایید نشده است	34
		شتاب در حال Sign Off است	86
رمز کارت را به صورت صحیح وارد شود	رمز کارت اشتباه وارد شده است	رمز کارت نادرست است	55
		عمل درخواستی پشتیبانی نمی‌شود	40
مبلغ خرید را حداقل 1000 ریال انتخاب نمایند	تراکنش خرید زیر 1000 ریال می‌باشد.	انجام تراکنش مورد درخواست توسط پایانه انجام دهنده مجاز نمی‌باشد/ تراکنش غیرمجاز	57
		انجام تراکنش مورد درخواست توسط پایانه انجام دهنده مجاز نمی‌باشد	58
ابتدا یک خرید 1000 ریالی انجام داده. از ساعت 12 ظهر به بعد، این مشکل در اولین ساعت زوج رفع می‌شود.	ناتوانی درگاه در تولید و ارسال Mac به سمت سوئیچ PSP	تمهیدات امنیتی نقض گردیده است/کلید MAC اشتباه است	63
مشکل مقطعی، سعی مجدد در زمان دیگر		اشکال در سیستم مرکزی	84
مشکل مقطعی، سعی مجدد در زمان دیگر	اشکال در سیستم مرکزی	قوانین سامانه نقض گردیده است، خطای داخلی سامانه/ اشکال در سیستم مرکزی	96
مشکل مقطعی، سعی مجدد در زمان دیگر		اشکال در حساب دارنده کارت	80
مشکل مقطعی، سعی مجدد در زمان دیگر	تراکنش برگشت خورده است.	تراکنش قبلا برگشت شده است	2
می‌بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.		تاریخ انقضا کارت سررسید شده است	54
می‌بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.	تعیین سقف مبلغ تراکنش خرید روزانه بر روی کارت	کارت محدود شده است	62
می‌بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.	رمز کارت بیش از 3 مرتبه بطور اشتباه وارد شده است.	تعداد دفعات ورود رمز اشتباه از حد مجاز فراتر رفته است	75
می‌بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.		اطلاعات کارت صحیح نمی‌باشد	14
موجودی حساب تامین شود	مبلغ مورد نظر در حساب دارنده کارت نیست.	موجودی حساب کافی نمی‌باشد	51
می‌بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.	کارت نامعتبر است	اطلاعات کارت یافت نشد/ اطلاعات کارت نامعتبر است	56



61	مبلغ تراکنش بیش از حد مجاز است/ محدودیت در مبلغ برداشت	مبلغ تراکنش از حد مجاز (سقف تعیین شده کارت) بیش تر است.	می بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.
65	تعداد دفعات انجام تراکنش بیش از حد مجاز است/اطلاعات کارت نا معتبر است	تعیین سقف تعداد تراکنش خرید روزانه بر روی کارت	می بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.
93	شلوغی سرور/تراکنش کامل نشد	ترافیک شبکه در سیستم بانکی (صادر کننده کارت)	می بایست تراکنش را مجدد و در زمان های مختلف تکرار نمایند.
92	کارت شتابی نمی باشد		می بایست تراکنش با کارت شتابی انجام شود.
91	زمان پاسخ بیش از حد مجاز	خطای ارتباطی	مبلغ طی 72 ساعت کاری به حساب دارنده کارت واریز میگردد. در صورت عدم واریز طی 72 ساعت، می بایست با سامانه 29911 تماس برقرار نماید.
90	تراکنش در زمان Cut Off انجام شده است		مبلغ طی 96 ساعت کاری به حساب دارنده درگاه واریز می شود.
78	کارت فعال نیست		در صورت عدم واریز طی 96 ساعت، به واحد مغایرت از طریق ثبت در پورتال مغایرت ارسال شود.
79	حساب متصل به کارت بسته یا دارای اشکال است		می بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.
42	کارت یا حساب مبدا در وضعیت پذیرش نمی باشد		می بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.
42	کارت یا حساب مقصد در وضعیت پذیرش نمی باشد		می بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.
31	عدم تطابق کد ملی خریدار با دارنده کارت		می بایست دارنده کارت به منظور پیگیری به بانک مراجعه نماید.
تراکنش با level 200	پذیرنده به دلیل انجام نشدن تراکنش با مرکز تماس ارتباط برقرار نموده و درخواست پیگیری دارند	چنانچه تراکنشی با level 200 در برتامه RMS مشاهده گردید می بایست به پذیرنده اعلام نمایید درحال حاضر امکان پیگیری این مورد مقدور نمی باشد و به جهت پیگیری مجدد 1 ساعت بعد تماس حاصل نمایند. و این مورد ثبت تماس شود	
98	سقف استفاده از رمز دوم ایستا به پایان رسیده است		سعی مجدد در روز مالی بعدی
عدم بروز رسانی درگاه	بررسی ورژن درگاه پرداخت اینترنتی		در صورتیکه درگاه با زمینه آبی باشد در گاه قدیمی میباشد و میبایست به روز رسانی گردد و مورد ثبت تماس میگردد.در صورتی



<p>که درگاه با زمینه سفید باشد در گاه به روز رسانی گردیده است و فاقد ایراد میباشد</p>			
<p>پایانه، شماره موبایل پذیرنده یا مسئول فنی سایت به همراه پیغام خطا از طریق outlook برای سوپروایزر ارسال شود.</p>	<p>1-ثبت نبودن IP سرور Host در سامانه MRS 2-تکراری بودن Invoice Number 3-غیر استاندارد بودن فرمت Amount یا مبلغ(مثل همراه داشتن ممیز) 4-اشتباه انتخاب کردن نام مقادیر پست شده به درگاه که باید کاملاً همانند فایل راهنما باشد که به بزرگ و کوچک بودن حروف نیز حساس می باشد.</p>		
<p>پایانه، شماره موبایل پذیرنده یا مسئول فنی سایت به همراه IP جدید از طریق تیکت ارجاع شود. (سطوح تیکت : سطح یک درگاه پرداخت اینترنتی - سطح دو افزودن / تغییر IP)</p>		<p>مواجه شدن با صفحه دسترسی غیر مجاز یا دریافت Token خالی</p>	<p>درخواست افزودن IP</p>
<p>پس از چک کردن و مشاهده تراکنش، نام فروشگاه و شماره تلفن ثابت در CRM به دارنده کارت داده می شود.(در صورتیکه دارنده کارت درخواست اطلاعات بیشتری را دارند می بایست درخواست خود را به مراجع قضایی، پلیس فتا و یا اداره آگاهی اعلام نمایند و فقط به درخواست های مکتوبی که از جانب سازمان های اعلامی به شرکت ارسال شوند پاسخ داده خواهد شد. نامه برای واحد دبیرخانه (فکس 85947401) ارسال گردد و در صورت پیگیری جواب نامه شماره 85947400 اعلام شود).</p>		<p>انجام تراکنش و درخواست دارنده کارت مبنی بر دریافت اطلاعات پذیرنده (دارنده درگاه)</p>	<p>اطلاعات درگاه اینترنتی</p>
<p>به دارنده کارت اعلام شود که به منظور پیگیری و برطرف شدن مشکل با پشتیبانی سایت مربوط تماس حاصل نمایند.</p>		<p>تماس دارنده کارت و اعلام پیغام خطا</p>	<p>اعلام پیغام خطا حین ورود یا پرداخت از درگاه پرداخت اینترنتی</p>
<p>پذیرنده راهنمایی شود، در سامانه گزارشات (MRS)، منوی مدیریت دسترسی پایانه و</p>		<p>درخواست پذیرنده</p>	<p>درخواست تغییر</p>



سپس گزینه بروزرسانی اطلاعات را انتخاب نمایید. در این قسمت پس از تایید گزینه open a file لوگوی جدید بارگذاری شود. پس از یک ساعت کاری لوگو تغییر خواهد یافت.			لوگوی درگاه
پس از دریافت اطلاعات (نام خانوادگی و شماره تماس پذیرنده) درخواست پذیرنده از طریق تیکت ارجاع شود. به پذیرنده توضیح داده شود که جهت هماهنگی از واحد درگاه با ایشان تماس حاصل خواهد شد.		درخواست پذیرنده	درخواست تغییر نام درگاه پرداخت اینترنتی
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری (اداره پشتیبانی نرم افزار) به منظور رفع مشکل		درخواست نامعتبر است (Tokenization)	901
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری (اداره پشتیبانی نرم افزار) به منظور رفع مشکل		پارامترهای اضافی درخواست نامعتبر می باشد (Tokenization)	902
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری (اداره پشتیبانی نرم افزار) به منظور رفع مشکل		شناسه پرداخت نامعتبر می باشد (Tokenization)	903
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری (اداره پشتیبانی نرم افزار) به منظور رفع مشکل		اطلاعات مرتبط با قبض نامعتبر می باشد (Tokenization)	904
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری (اداره پشتیبانی نرم افزار) به منظور رفع مشکل		شناسه درخواست نامعتبر می باشد (Tokenization)	905
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری (اداره پشتیبانی نرم افزار) به منظور رفع مشکل		درخواست تاریخ گذشته است (Tokenization)	906
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری (اداره پشتیبانی نرم افزار) به منظور رفع مشکل		آدرس بازگشت نتیجه پرداخت نامعتبر می باشد (Tokenization)	907
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری (اداره پشتیبانی نرم افزار) به منظور رفع مشکل		پذیرنده نامعتبر می باشد (Tokenization)	909
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری (اداره پشتیبانی نرم افزار) به منظور رفع مشکل		پارامترهای مورد انتظار پرداخت تسهیمی تامین نگردیده است (Tokenization)	910



ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		پارامترهای مورد انتظار پرداخت تسهیمی نا معتبر یا دارای اشکال می باشد (Tokenization)	911
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		تراکنش درخواستی برای پذیرنده فعال نیست (Tokenization)	912
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		تراکنش تسهیم برای پذیرنده فعال نیست (Tokenization)	913
پایانه، شماره موبایل پذیرنده یا مسئول فنی سایت به همراه IP صحیح از طریق تیکت ارجاع شود. سطوح تیکت : سطح یک درگاه پرداخت اینترنتی- سطح دو افزودن / تغییر IP	مشکل IP	آدرس آی پی دریافتی درخواست نا معتبر می باشد	914
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		شماره پایانه نامعتبر می باشد (Tokenization)	915
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		شماره پذیرنده نا معتبر می باشد (Tokenization)	916
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		نوع تراکنش اعلام شده در خواست نا معتبر می باشد (Tokenization)	917
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		پذیرنده فعال نیست (Tokenization)	918
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		مبالغ تسهیمی ارائه شده با توجه به قوانین حاکم بر وضعیت تسهیم پذیرنده ، نا معتبر است (Tokenization)	919
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		شناسه نشانه نامعتبر می باشد	920
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		شناسه نشانه نامعتبر و یا منقضی شده است	921
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		نقض امنیت درخواست (Tokenization)	922



ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		ارسال شناسه پرداخت در تراکنش قبض مجاز نیست (Tokenization)	923
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		مبلغ مبادله شده نا معتبر می باشد (Tokenization)	928
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		شناسه پرداخت ارائه شده با توجه به الگوریتم متناظر نا معتبر می باشد (Tokenization)	929
ارسال کد خطا از طریق تیکت توسط مرکز تماس به مدیریت عملیات و راهبری(اداره پشتیبانی نرم افزار) به منظور رفع مشکل		کد ملی ارائه شده نا معتبر می باشد (Tokenization)	930
	اطلاعات ارسالی در RevertUri دارای host یکسان با Host مندرج در وب سایت ثبت شده پذیرنده نمی باشد	MerchantAndRevertUriMustHaveSameHost	936
کد ملی رمز شده وجود ندارد.		InvalidEncNationalId	937



۱۲ کوتاه نوشت ها

ردیف	کوتاه نوشت	توضیحات
1	..17	طول متغیر تا حداکثر 17 کاراکتر ، عدد مربوطه مشخص کننده حد اکثر طول مجاز رشته می باشد
2	3	طول ثابت، عدد مربوطه طول ثابت را نمایان می سازد
3	a	مجموعه ای از حروف انگلیسی یا فارسی بر اساس کدینگ UTF-8
4	n	مجموعه ای از اعداد 0-9
5	an	مجموعه ای از حروف انگلیسی یا فارسی بر اساس کدینگ UTF-8 و کاراکترهای 0-9
6	ans	مجموعه ای از حروف انگلیسی و کاراکترهای خاص بر اساس کدینگ UTF-8 و کاراکترهای 0-9
7	h	مجموعه از کاراکترهای A-F و 0-9
8	b	مجموعه ای از داده های دودویی که در مبنای HEX ارسال می گردد
9	obj	یک شی JSON که خود شامل یک یا چند پارامتر دیگر است
10	obj(x)	یک شی JSON که پارامترهای تشکیل دهنده آن در کلاس X مشخص شده است
11	array	یک آرایه از یک شی JSON
12	array(x)	یک آرایه از یک شی JSON که پارامترهای تشکیل دهنده آن در کلاس X مشخص گردیده است
13	s(n)	رشته است شامل حروف 0-9
14	Y	بلی (اجباری)
15	N	خیر
16	O	اختیاری
17	C	مشروط