شاپرک
شرکت شبکه الکترونیکی پرداخت کارت (سهامی خاص)

ضوابط و مقررات شاپرک

پروتکل وب سرویس‌های درخواست‌رمز یکبار مصرف جهت انجام تراکنش های غیر حضوری

جهت پیاده‌سازی توسط فن‌آوران مالی (پرداخت سازان)

کد مستند: SHP_INS_FINTECHOTPREQUEST

ویرایش: 01-01

۱۳۹۸/۰۹/۲۷

بسم الله الرحمن الرحیم

شناسنامه‌ی مستند	
نگارنده	شبکه الکترونیکی پرداخت کارت-شاپرک
عنوان مستند	پروتکل وب سرویس‌های درخواست‌رمز یکبار مصرف جهت انجام تراکنش های غیر حضوری
کد مستند	SHP_INS_FINTECHOTPREQUEST
شماره ویرایش	01-01
تاریخ تدوین/بازنگری	۱۳۹۸/۰۹/۲۷
تاریخ اجرا	بلافاصله پس از ابلاغ
تاریخ مؤثر سند	بلافاصله پس از ابلاغ
جامعه هدف	فن‌آوران مالی (پرداخت‌سازان)
مراجع	-
	-
	-
مدارک ذیربط	ندارد.

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

کنترل نسخ مستندات

شماره ویرایش	موضوع بازنگری	تاریخ بازنگری	نگارنده
۰۱-۰۱	اضافه‌شدن بخش الزامات فرایندی استفاده از برنامه کاربردی	۹۸/۰۹/۲۷	شاپرک

جدول ثبت تغییرات مدرک (مربوط به آخرین نسخه)

شماره تغییر	صفحه	محل تغییر	تغییرات اعمال شده	تاریخ بازنگری	نگارنده
۰۱	۱۸	بند ۵-۵	بخش مربوط به الزامات فرایندی استفاده از برنامه کاربردی	۹۸/۰۹/۲۷	شاپرک

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

فهرست مطالب

۱- مقدمه ۷
۲- اهداف ۷
۳- کاربران ۷
۴- تعاریف ۷
۴-۱- شرکت شاپرک ۷
۴-۲- پرداخت ساز ۷
۴-۳- سامانه هریم (هدایت رمز یکبار مصرف) ۷
۴-۴- بانکهای صادرکننده کارت عضو شبکه شتاب ۸
۵- شرح ۸
۵-۱- ساختار کلی سرویس‌ها ۸
۵-۱-۱- کوته واژه های مورد استفاده در مستند ۹
۵-۱-۲- ساختار کلی پیام‌های درخواست ۱۰
۵-۱-۳- ساختار کلی پیام‌های پاسخ ۱۱
۵-۲- سرویس درخواست دریافت رمز یکبار مصرف ۱۳
۵-۳- امنیت وب سرویس ۱۵
۵-۴- جداول پایه ۱۶
۵-۴-۱- جدول انواع کانال ارسال رمز یکبار مصرف ۱۶
۵-۴-۲- جدول انواع فاکتورهای امنیتی ۱۶
۵-۴-۳- جدول وضعیت درخواست ۱۶
۵-۴-۴- جدول انواع ترمینال ۱۶
۵-۴-۵- جدول انواع تراکنش ۱۷
۵-۴-۶- جدول کدهای خطا ۱۷
۵-۵- الزامات فرایندی استفاده از برنامه کاربردی موبایلی ۱۸
۵-۵-۱- اطلاعات مجاز قابل دریافت در برنامه کاربردی موبایلی ۱۸
۵-۵-۲- رعایت الزامات امنیتی ۲۰
۵-۶- پیوست- نمونه اقلام اطلاعاتی مندرج در برنامه‌های کاربردی موبایلی ۲۱

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

فهرست جداول

جدول ۱: انواع اقلام دادهای ۹
جدول ۲: ساختار کلی پیام‌های درخواست ۱۰
جدول ۳: ساختار کلی پیام پاسخ عملیات مالی ۱۱
جدول ۴: ساختار اطلاعات کانال ارسال ۱۱
جدول ۵: ساختار لیست خطا ۱۲
جدول ۶: ساختار پیام درخواست دریافت رمز یکبار مصرف ۱۳
جدول ۷: ساختار پاسخ به درخواست دریافت رمز یکبار مصرف ۱۴
جدول ۸: انواع کانال رمز یکبار مصرف ۱۶
جدول ۹: انواع فاکتورهای امنیتی ۱۶
جدول ۱۰: وضعیت درخواست ۱۶
جدول ۱۱: انواع پایانه ۱۶
جدول ۱۲: انواع تراکنش ۱۷
جدول ۱۳: کدهای خطا ۱۸

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

فهرست پیام‌ها

پیام ۱: نمونه JSON لیست خطا ۱۲
پیام ۲: نمونه JSON لیست خطا ۱۲
پیام ۳: نمونه JSON درخواست دریافت رمز یکبار مصرف ۱۴
پیام ۴: نمونه JSON پاسخ سرویس درخواست دریافت رمز یکبار مصرف ۱۵

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

۱- مقدمه

مستند فنی سامانه درخواست رمز یکبار مصرف، مجموعه‌ای از تعاریف، قراردادها، مفاهیم و ساختار اطلاعات تبادلی بین شرکت شبکه الکترونیک پرداخت کارت (شاپرک) و فن‌آوران مالی (پرداخت‌سازان) می‌باشد. لذا به منظور یکپارچگی و حفظ امنیت تبادل پیام‌ها و تراکنش‌های مالی، مستند حاضر تهیه و در اختیار فن‌آوران مالی فعال در حوزه پرداخت‌سازی قرار گرفته است.

۲- اهداف

هدف از تدوین این مستند، ارائه روشی یکپارچه و امن به منظور پیاده‌سازی پروتکل ارتباطی بین شبکه الکترونیکی پرداخت کارت و فن‌آوران مالی می‌باشد. فن‌آوران مالی (پرداخت‌سازان) به منظور فراهم آوردن امکان درخواست دریافت رمز یکبار مصرف توسط دارندگان کارت جهت انجام تراکنش‌های کارتی غیرحضوری، پروتکل توضیح داده شده در این مستند را پیاده‌سازی نموده و از طریق واسط کاربری سامانه‌های پرداخت در اختیار دارندگان کارت قرار می‌دهند.

۳- کاربران

کاربران این سند، فن‌آوران مالی متقاضی پرداخت‌سازی می‌باشند.

۴- تعاریف

۴-۱- شرکت شاپرک

شبکه الکترونیکی پرداخت کارت «شاپرک»، شبکه‌ای است که به منظور ساماندهی نظام پرداخت در کشور ایجاد شده و کلیه تراکنش‌های حاصل از «ابزارهای پذیرش» توسط این شبکه نظارت و کنترل می‌شود و به طور کلی نظارت بر عملکرد فنی و اجرایی را برعهده دارد.

۴-۲- پرداخت ساز

شخصیت حقوقی که با توسعه برنامک، امکان آغاز و تجمیع تراکنش‌های انتقال وجه کارت به کارت را فراهم آورده و درچارچوب الزامات و مقررات بانک مرکزی ج.ا.ا. در این حوزه فعالیت می‌نماید.

۴-۳- سامانه هریم (هدایت رمز یکبار مصرف)

سامانه‌ای است برای هدایت رمز یکبار مصرف که از طریق آن می‌توان درخواست رمز یکبار مصرف را به صادرکننده کارت ارسال کرد.

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

۴-۴- بانک‌های صادرکننده کارت عضو شبکه شتاب

تمامی بانک‌ها و موسسات مالی و اعتباری صادرکننده کارت که از طرف شبکه شتاب به رسمیت شناخته شده و امکان اتصال، ایجاد و دریافت تراکنش بر بستر این شبکه را دارند.

۵- شرح

از این سامانه جهت مدیریت و ارسال درخواست‌های دریافت رمز یکبار مصرف، به بانک‌های صادر کننده کارت، جهت آغاز تراکنش‌های غیرحضوری استفاده می‌شود.

۵-۱- ساختار کلی سرویس‌ها

کلیه سرویس‌ها به صورت RESTFUL ارائه گردیده و فراخوانی آنها به صورت POST می‌باشد. محتوا با فرمت JSON و در قالب Request Body ارسال می‌گردد و خروجی سرویس‌ها نیز با فرمت JSON در Response Body بازخواهد گشت. همچنین آدرس‌های ارائه شده به صورت نسبی (Relative) می‌باشند و با برقراری ارتباط شبکه‌ای آدرس پایه ارائه شده توسط شرکت شاپرک به ابتدای آدرس‌های نسبی داده شده اضافه می‌گردد.

علاوه بر موارد اصلی بالا، نکات ذیل پیرو پیاده‌سازی کلی فنی وب سرویس‌ها قابل ذکر است:

- لازم است در تمامی موارد قالب Stringهای ارسالی از سمت کلاینت و سرور UTF-8 باشد.
- منظور از Timestamp تعداد هزارم ثانیه (Millisecond) های سپری شده از تاریخ مبدا ۱۹۷۰/۰۱/۰۱ میلادی به مرجع UTC می‌باشد که همواره به صورت عددی ارائه می‌گردد. این عدد برای تاریخ‌های پیش از مبدا یاد شده به صورت منفی ارائه می‌گردد.
- در این مستند مرجع اصلی پیاده‌سازی، جداول بوده و نمونه JSONهای ارائه شده صرفا جنبه اطلاعات تکمیلی دارند.
- چنانچه ورودی‌های ارائه‌شده از نظر قالب JSON معتبر نباشند (قابل Deserialize کردن نباشند)، یا مقادیر داده شده برای فیلدهای Enum خارج از مقادیر معتبر ارائه شده در مستند باشند، یا مقدار داده شده برای فیلدی خارج از قالب اعلام شده در مستند باشد (به عنوان مثال برای فیلدی از جنس String مقداری از نوع Number ارائه گردد) و یا فیلدی با نام ناشناخته به هنگام فراخوانی ارائه گردد، لازم است سرویس‌دهنده بدون پردازش منطقی درخواست، کد پاسخ HTTP ۴۰۰ (Bad Request) باز گرداند و در بدنه پاسخ نیز حتی‌الامکان داده دارای خطا را مشخص نماید. در این

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

حالت خاص، قالبی برای پاسخ وجود نداشته و صرفا ارائه اطلاعات کافی درمورد منشا خطا به صورت plain text به سرویس‌گیرنده ارسال خواهد گشت.

- در حالتی که سرویس‌دهنده با خطای داخلی غیر منطقی Handle نشده مواجه می‌گردد، کد پاسخ HTTP ۵۰۰ باز می‌گرداند. با این حال در حد امکان برای تمامی خطاهایی که به صورت منطقی قابل اعتبار سنجی باشند، خطاهای منطقی قابل تفسیر سیستمی متناسب با قالب داده شده در مستند بازگردانده می‌شوند.
- به جز سه حالت مطرح شده در مستند که کد های پاسخ ۴۰۰، ۴۰۱ و ۵۰۰مطابق استاندارد HTTP بازگردانده می‌شود، در تمامی حالات کد پاسخ ۲۰۰ به همراه پاسخی در قالب ارائه شده در مستند بازگردانده خواهد شد. لازم به ذکراست در حالاتی که کد پاسخ غیر از ۲۰۰ بازگردانده می‌شود، قالب خاصی جهت خروجی وجود ندارد، با این حال در حالت ۴۰۰، داده‌های ارائه شده در بدنه پاسخ جهت تشخیص کلی خطا به صورت غیرسیستمی (انسانی) کفایت می‌کند.

۵-۱-۱- کوته واژه های مورد استفاده در مستند

با توجه به اینکه در ساختار پیش‌بینی شده، صرفا شش نوع کلی داده وجود خواهد داشت، در جداول زیر اقلام اطلاعاتی رشته‌ای به اختصار S[۱]، اقلام اطلاعاتی عددی به اختصار N[۲]، اقلام اطلاعاتی دو انتخابی (بولی) به اختصار B[۳]، اقلام اطلاعاتی Timestamp (شامل تاریخ و زمان) که دقت آن تا هزارم ثانیه می‌باشد به اختصار T، اشیاء که خود شامل تعدادی فیلدهای اطلاعاتی می‌باشند به اختصار O[۴] و فیلدهای آرایه‌ای که شامل مجموعه‌ای از سایر اقلام اطلاعاتی می‌باشند، به اختصار A[۵] در جداول نمایش داده شده است.

ردیف	اختصار	عنوان
۱	S	رشته
۲	N	عدد
۳	B	دو انتخابی (بولی)
۴	T	تاریخ و زمان
۵	O	شیء
۶	A	آرایه

جدول ۱: انواع اقلام داده‌ای

[۱] Sting
[۲] Number
[۳] Boolean
[۴] Object
[۵] Array

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

لازم به ذکر است برای اقلام اطلاعاتی رشته‌ای یا عددی در داخل پرانتز حداقل و حداکثر طول قابل قبول فیلدهای اطلاعاتی نیز ذکر گردیده است. به عنوان مثال اگر فیلد شماره رهگیری یک فیلد رشته‌ای که حداقل طول آن ۸ کاراکتر و حداکثر طول آن ۶۴ کاراکتر باشد، به اختصار S(8,64) درجدول نمایش داده می‌شود.

۵-۱-۲- ساختار کلی پیام‌های درخواست

در این بخش اقلام اطلاعاتی مورد استفاده در پیام‌های مرتبط با درخواست و ارائه رمز یکبار مصرف به اختصار تشریح می‌گردد و در ادامه این مستند هر یک از انواع پیام با جزئیات ساختار و نمونه پیام توضیح داده خواهد شد.

ساختار کلی اقلام اطلاعاتی در پیام‌های درخواست (ورودی وب سرویس‌ها) به شرح ذیل می‌باشد:

ردیف	نام فیلد	نام فارسی	نوع فیلد	توضیحات
۱	acceptorCode	شماره پذیرنده	S(15,15)	شماره پذیرنده در این فیلد درج می‌گردد.
۲	acceptorName	نام پذیرنده	S(1,50)	نام پذیرنده (فروشگاه) در این فیلد درج می‌گردد.
۳	accessAddress	آدرس فراخوانی پایانه	S(7,15)	آدرس درخواست کننده اصلی رمز یکبار مصرف
۴	amount	مبلغ	N(1,12)	مبلغ تراکنش در این فیلد درج می‌گردد.
۵	rrn	شماره مرجع بازیابی تراکنش	S(1,12)	شماره مرجع بازیابی تراکنش در این فیلد درج می‌گردد.
۶	securityFactor	فاکتور امنیتی	S(16,512)	بسته به مقدار فیلد "نوع فاکتور امنیتی"، داده های این فیلد با الگوریتم مناسب تولید شده و در این فیلد قرار می گیرد.
۷	securityType	نوع فاکتور امنیتی	N(1,1)	روش تضمین اصالت/امنیت/انکار ناپذیری پیام مطابق با جدول شماره ۹
۸	sourcePAN	شماره کارت/شاخص کارت مبدا	S(16,19)	شماره کارت/شاخص کارت مبدا تراکنش در این فیلد درج می‌گردد.
۹	stan	شماره پیگیری تراکنش	N(1,6)	شماره پیگیری تراکنش در این فیلد درج می‌گردد.
۱۰	terminalNumber	شماره پایانه	S(8,8)	شماره پایانه در این فیلد درج می‌گردد.
۱۱	terminalType	نوع پایانه	N(1,1)	نوع پایانه مطابق با جدول شماره ۱۱ در این فیلد درج می‌گردد.
۱۲	trackingNumber	شماره رهگیری درخواست	S(8,64)	شماره رهگیری درخواست در این فیلد درج می‌گردد.
۱۳	transactionType	نوع تراکنش	N(1,1)	نوع تراکنش در این فیلد مطابق با جدول شماره ۱۲درج می‌گردد.

جدول ۲: ساختار کلی پیام‌های درخواست

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

۵-۱-۳- ساختار کلی پیام‌های پاسخ

به طور کلی ساختار پیام‌های پاسخی که در جواب درخواست‌ها ارسال می‌گردند، در این بخش توضیح داده می‌شود. لازم به ذکر است ساختار اشیاء پیچیده (Composite) موجود در پیام‌های پاسخ در جداول بعدی توضیح داده می‌شوند.

ساختار کلی فیلدهای موجود در پیام‌های پاسخ به شرح ذیل می‌باشد:

ردیف	نام فیلد	نام فارسی	نوع فیلد	توضیحات
۱	deliveryChannels	لیست کانال های ارسال رمز	A[DeliveryChannel]	لیست کانال‌های ارسال رمز یکبار مصرف برای دارنده کارت در این فیلد مطابق جدول شماره ۴ درج می گردد.
۲	errors	لیست خطاها	A[Error]	لیست خطاها شامل مجموعه‌ای از اشیاء خطا (error) مطابق با جدول شماره ۵ تکمیل می‌گردد.
۳	registrationDate	تاریخ ثبت درخواست	T	تاریخ ثبت درخواست در سمت سرور در این فیلد درج می گردد.
۴	requestId	شناسه درخواست	S(8,64)	شناسه یکتای درخواست در این فیلد درج می‌گردد.
۵	status	وضعیت درخواست	N(1,1)	وضعیت درخواست مطابق با جدول شماره ۱۰ تکمیل می‌گردد.
۶	trackingNumber	شماره رهگیری درخواست	S(8,64)	شماره رهگیری درخواست در این فیلد درج می‌گردد.

جدول ۳: ساختار کلی پیام پاسخ عملیات مالی

۵-۱-۳-۱- ساختار شیء اطلاعات کانال ارسال

در این بخش جزئیات فیلدهای اطلاعاتی مربوط به شیء (object) اطلاعات کانال ارسال (DeliveryChannel) در جدول ذیل ارایه می‌گردد.

ردیف	نام فیلد	نام فارسی	نوع فیلد	توضیحات	اجباری/ اختیاری
۱	channelAdditionalData	داده‌های اضافی کانال	S(1,99)	داده‌های اضافی مربوط به کانال ارسال رمز یکبار مصرف در این فیلد درج می‌گردد.	M
۲	channelType	نوع کانال	N(1,1)	نوع کانال ارسال رمز یکبار مصرف در این فیلد مطابق با جدول شماره ۸ درج می‌گردد.	M

جدول ۴: ساختار اطلاعات کانال ارسال

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

نمونه JSON لیست لیست کانال های ارسال رمز در پیام های پاسخ :

```
{
  "deliveryChannels": [
    {
      "channelType": 0,
      "channelAdditionalData": "0912*****20"
    }
  ]
}
```

پیام ۱: نمونه JSON لیست خطا

۵-۱-۳-۲- ساختار شیء خطا

با توجه به اینکه ساختار لیست خطا در پاسخ تمامی سرویس‌ها یکسان می‌باشد در این بخش جزئیات فیلدهای اطلاعاتی مربوط به شیء (object) خطا (Error) در جدول ذیل ارایه می‌گردد و در ادامه مستند از تکرار این بخش امتناع می‌گردد.

ردیف	نام فیلد	نام فارسی	نوع فیلد	توضیحات	اجباری/ اختیاری
۱	errorCode	کد خطا	N(1,3)	مطابق با جدول شماره ۱۳تکمیل می‌گردد.	M
۲	errorDescription	شرح خطا	S(1,256)	شرح خطا	M
۳	referenceName	نام فیلد/ هویت	S(1,256)	نام فیلد/ هویتی است که خطا ناشی از آن می‌باشد.	O
۴	originalValue	مقدار منجر به خطا	S(1,256)	مقدار ارسالی است که منجر به ایجاد خطا گردیده است.	O
۵	extraData	اطلاعات اضافی	S(1,256)	سایر اطلاعات اضافی مرتبط با خطا در این فیلد ذکر می‌گردد.	O

جدول ۵: ساختار لیست خطا

نمونه JSON لیست خطاها در پیام های پاسخ :

```
{
  "errors": [
    {
      "errorCode": 1,
      "errorDescription": "Mandatory field not set",
      "referenceName": "amount",
      "originalValue": null,
      "extraData": ""
    }
  ]
}
```

پیام ۲: نمونه JSON لیست خطا

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

۵-۲- سرویس درخواست دریافت رمز یکبار مصرف

مسیر دسترسی:

/tansfer/requestOtp

هدف از این سرویس امکان درخواست دریافت رمز یکبار مصرف توسط دارنده کارت می باشد.

ورودی این سرویس از جنس object درخواست دریافت رمز یکبار مصرف (**OtpDeliveryRequest**) بوده و خروجی آن نیز به صورت object پاسخ به درخواست دریافت رمز یکبار مصرف (**OtpDeliveryResponse**) می‌باشد.

ساختار object درخواست دریافت رمز یکبار مصرف مطابق جدول زیر می‌باشد:

ردیف	نام فیلد	نام فارسی	توضیحات	اجباری/ اختیاری
۱	trackingNumber	شماره رهگیری درخواست	شماره رهگیری درخواست توسط شرکت های پرداخت تولید می گردد و لازم است در سطح شرکت یکتا باشد.	M
۲	sourcePAN	شماره کارت/شاخص کارت مبدا	شماره کارتی که رمز یکبار مصرف برای آن درخواست شده است.	M
۳	amount	مبلغ تراکنش	عینا مبلغی که از طریق پایانه به کاربر نمایش داده می شود.	M
۴	transactionType	نوع تراکنش	نوع تراکنش مطابق با جدول ۱۲تکمیل می گردد.	M
۵	acceptorCode	شماره پذیرنده	شماره پذیرنده ایجاد کننده تراکنش	M
۶	acceptorName	نام پذیرنده	نام پذیرنده ایجاد کننده تراکنش	M
۷	terminalNumber	شماره پایانه	شماره پایانه ایجاد کننده تراکنش	M
۸	terminalType	نوع پایانه	نوع پایانه ایجاد کننده تراکنش مطابق با جدول شماره ۱۱	M
۹	rrn	شماره مرجع بازیابی تراکنش	شماره مرجع بازیابی تراکنش که در هنگام استعلام نام دارنده کارت مقصد دریافت شده است، در این فیلد بازگردانده می شود.	O
۱۰	stan	شماره پیگیری تراکنش	شماره پیگیری تراکنش که در هنگام استعلام نام دارنده کارت مقصد دریافت شده است، در این فیلد بازگردانده می شود.	O
۱۱	accessAddress	آدرس فراخوانی پایانه	در پایانه های اینترنتی با آدرس IP درخواست کننده اصلی و در تراکنش های USSD با شماره تلفن همراه فراخوانی کننده تکمیل می گردد.	M
۱۲	securityType	نوع فاکتور امنیتی	نوع فاکتور امنیتی مورد استفاده جهت تصدیق و تضمین امنیت پیام مطابق با جدول شماره ۹	M
۱۳	securityFactor	فاکتور امنیتی	فاکتور امنیتی جهت تصدیق و تضمین امنیت پیام	O

جدول ۶: ساختار پیام درخواست دریافت رمز یکبار مصرف

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

نمونه JSON ورودی سرویس درخواست دریافت رمز یکبار مصرف:

```
{
  "trackingNumber": "45ggfhfgh54tfg45-dfsdf",
  "sourcePAN": "XXXXXXXXXXXXXXXX",
  "amount": 10000.0,
  "transactionType": 0,
  "acceptorCode": "123456789012345",
  "acceptorName": "پذیرنده تستی",
  "terminalNumber": "12345678",
  "terminalType": 1,
  "rrn": "123456789012",
  "stan": 123456,
  "accessAddress": "192.168.0.1",
  "securityType": 1,
  "securityFactor":
"bRYuwenvDemYW7OWDoQ4vGNKJ0/rNXDP5zumrWhSurdTneAqV0nvjs59J/0F0V1F+7Ki4OdPQ5Z
puInlsf+Z+6ea7zofN4ybECF99FMhINyIxNGNiWkdeHNitRr80qaFx5Uri8cmPIrAmgJaMXmkuSq
g6pGr/qrnInKXRij2FYY="
}
```

پیام ۳: نمونه JSON درخواست دریافت رمز یکبار مصرف

ساختار object پاسخ به درخواست دریافت رمز یکبارمصرف مطابق جدول زیر می‌باشد:

ردیف	نام فیلد	نام فارسی	توضیحات	اجباری/ اختیاری
۱	trackingNumber	شماره رهگیری درخواست	شماره رهگیری درخواست که در فرآیند ثبت درخواست ارایه شده، در این فیلد بازگردانده می شود.	M
۲	status	وضعیت درخواست	وضعیت درخواست مطابق با جدول شماره ۱۰ تکمیل می‌گردد.	M
۳	requestId	شناسه درخواست	درصورت پذیرش موفق درخواست، این فیلد به عنوان شناسه یکتا درخواست تکمیل می‌گردد.	O
۴	registrationDate	تاریخ ثبت درخواست	درصورت پذیرش موفق درخواست، تاریخ ثبت درخواست در این فیلد درج می‌گردد.	O
۵	deliveryChannels	لیست کانال های ارسال رمز	لیست کانال‌های استفاده شده جهت ارسال رمز یکبار مصرف درخواست شده در این فیلد درج می‌گردد.	O
۶	errors	لیست خطاها	در صورت عدم پذیرش درخواست، لیست خطاهای منطقی در این فیلد درج می‌گردد.	O

جدول ۷: ساختار پاسخ به درخواست دریافت رمز یکبار مصرف

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

نمونه JSON خروجی سرویس درخواست دریافت رمز یکبار مصرف :

```
{
  "trackingNumber": "45ggfhfgh54tfg45-dfsdf",
  "status": 1,
  "requestId": "dfg5645trdghui56-dfg",
  "registrationDate": 1570457495723,
  "deliveryChannels": [
    {
      "channelType": 0,
      "channelAdditionalData": "0912*****20"
    }
  ],
  "errors": []
}
```

پیام ۴: نمونه JSON پاسخ سرویس درخواست دریافت رمز یکبار مصرف

۵-۳- امنیت وب سرویس

جهت اطمینان از امنیت استفاده از وب‌سرویس، در کنار موارد مربوط به امنیت کانال از قبیل IP، SSL Encryption Restriction و VPN Tunnel، که بنابر توافق و نیازمندی از سمت سرویس‌دهنده (شرکت شاپرک) اعمال می‌گردند، نیاز است تا سرویس‌گیرنده (فن‌آوران مالی) نیز در هنگام فراخوانی سرویس، اطلاعات مربوط به تصدیق هویت- اعم از نام کاربری و کلمه عبور- را در Header درخواست ارسال نمایند.

قالب ارسال اطلاعات تصدیق هویت مطابق استاندارد Basic Access Authentication (BA) و به شرح زیر خواهد بود:

۱. رشته‌ای از نام کاربری و کلمه عبور که با دو نقطه (:) از هم جدا شده‌اند ایجاد می‌گردد.

<user_name>:<password>

۲. رشته تولید شده در بند قبل به قالب Base64 تبدیل می‌گردد بعنوان نمونه:

PHVzZXJfbmFtZT46PHBhc3N3b3JkPg==

۳. نتیجه با کلید Authorization و با یک فاصله پس از کلمه کلیدی Basic در Header درخواست ارسال می‌گردد بعنوان نمونه:

Authorization: Basic PHVzZXJfbmFtZT46PHBhc3N3b3JkPg==

لازم به ذکر است سرویس دهنده نیز موظف است مطابق استاندارد BA، در وضعیت خطای Authentication، کد پاسخ ۴۰۱ به همراه Headerهای مناسب را برگرداند.

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

۵-۴- جداول پایه

۵-۴-۱- جدول انواع کانال ارسال رمز یکبار مصرف

ردیف	مقدار	عنوان	توضیحات
۱	۰	پیامک	ارسال پیامک به شماره موبایل دارنده کارت
۲	۱	ایمیل	ارسال ایمیل به دارنده کارت
۳	۲	تماس تلفنی	برقراری تماس تلفنی با شماره تلفن دارنده کارت
۴	۳	برنامک موبایلی	ارسال به برنامه موبایلی دارنده کارت
۵	۴	اینترنت بانک	ارسال رمز عبور به اینترنت بانک صادرکننده کارت
۶	۵	رمز ثابت	استفاده از رمز دوم ثابت

جدول ۸: انواع کانال رمز یکبار مصرف

۵-۴-۲- جدول انواع فاکتورهای امنیتی

ردیف	مقدار	عنوان	توضیحات
۱	۰	عدم استفاده از فاکتور امنیتی	عدم استفاده از فاکتور امنیتی
۲	۱	امضاء دیجیتال	استفاده از امضای دیجیتال
۳	۲	MAC	استفاده از تصدیق هویت پیام

جدول ۹: انواع فاکتورهای امنیتی

۵-۴-۳- جدول وضعیت درخواست

ردیف	مقدار	عنوان	توضیحات
۱	۰	عدم پذیرش	عدم پذیرش موفق درخواست رمز یکبار مصرف
۲	۱	پذیرش موفق	پذیرش موفق درخواست رمز یکبار مصرف

جدول ۱۰: وضعیت درخواست

۵-۴-۴- جدول انواع ترمینال

ردیف	مقدار	عنوان	توضیحات
۱	۱	Internet Payment Gateway/Web App	پایانه اینترنتی
۲	۵	Mobile App	اپلیکیشن موبایلی
۳	۶	Mobile SDK	کتابخانه توسعه نرم افزار موبایلی
۴	۷	Exposed API	سرویس برون سپاری شده

جدول ۱۱: انواع پایانه

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

۵-۴-۵- جدول انواع تراکنش

ردیف	مقدار	عنوان
۱	۰	انتقال وجه
۲	۱	درخواست مانده حساب
۳	۲	درخواست چکیده صورتحساب
۴	۳	پرداخت قبض
۵	۴	خرید شارژ
۶	۵	درخواست تایید رمز کارت

جدول ۱۲: انواع تراکنش

۵-۴-۶- جدول کدهای خطا

ردیف	مقدار	عنوان
۱	۰	خطای عمومی (جزئیات مرتبط در referenceName و extraData ذکر می‌گردد.)
۲	۱	عدم ارسال مقدار برای فیلد اجباری (نام فیلد/هویت مربوطه عینا در referenceName ذکر می‌گردد.)
۳	۲	قالب منطقی یا check digit نادرست داده ارسالی (نام فیلد/هویت مربوطه عینا در referenceName ذکر می‌گردد.)
۴	۳	ارسال داده تکراری (عنوان فیلد/هویت محتوی داده‌های تکراری عینا در referenceName ذکر می‌گردند.)
۵	۴	عدم همخوانی بین داده‌های ارائه شده (نام فیلدهای مغایر عینا در referenceName ذکر می‌گردند و با ":" از هم جدا می‌شوند.)
۶	۵	عدم همخوانی داده ارائه شده با قراردادهای سرویس (نام فیلد/هویت مربوطه عینا در referenceName ذکر می‌گردد.)
۷	۶	عدم وجود داده مورد اشاره (نام فیلد/هویت مربوطه عینا در referenceName ذکر می‌گردد.)
۸	۷	عدم وجود منابع کافی جهت تکمیل درخواست (نام منبع – برای مثال balance – در referenceName ذکر می‌گردد.)
۹	۸	عدم دسترسی سرویس‌گیرنده به داده مورد ارجاع (نام فیلد/هویت مربوطه عینا در referenceName ذکر می‌گردد.)
۱۰	۹	عدم امکان برداشت/واریز (نام فیلد/هویت مربوطه عینا در referenceName ذکر می‌گردد.)
۱۱	۱۰	امکان فراخوانی سرویس به صورت موقت وجود ندارد
۱۲	۱۱	خطای داخلی سیستم سرویس‌دهنده
۱۳	۱۲	عدم دسترسی موقتی به سرویس بیرونی
۱۴	۱۳	عدم دریافت پاسخ از سرویس بیرونی

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

ردیف	مقدار	عنوان
۱۵	۱۴	نیاز به ارسال مجدد درخواست می‌باشد
۱۶	۱۵	عدم امکان ارائه سرویس درخواستی
۱۷	۱۶	خطای امنیتی (نام فیلد/هویت محتوی داده مربوطه عینا در referenceName ذکر می‌گردد.)
۱۸	۱۷	داده خارج از محدوده مورد قبول (نام فیلد/هویت محتوی داده مربوطه عینا در referenceName ذکر می‌گردد.)
۱۹	۱۸	مرجع غیر فعال (نام فیلد/هویت محتوی داده مربوطه عینا در referenceName ذکر می‌گردد.)
۲۰	۱۹	انقضاء/ابطال مرجع مورد اشاره (نام فیلد/هویت محتوی داده مربوطه عینا در referenceName ذکر می‌گردد.)

جدول ۱۳: کدهای خطا

۵-۵- الزامات فرایندی استفاده از برنامه کاربردی موبایلی

فناوران مالی به منظور ارائه خدمت از طریق برنامه کاربردی موبایلی، موظف به رعایت الزامات زیر می‌باشند:

۵-۵-۱- اطلاعات مجاز قابل دریافت در برنامه کاربردی موبایلی

در ارائه خدمت از طریق برنامه کاربردی موبایلی تنها دریافت اطلاعات به شرح زیر مجاز می‌باشد:

- شماره کارت
- رمز دوم
- شماره شناسایی دوم (CVV2)
- تاریخ انقضای کارت

نکته ۱: پس از تکمیل فیلد شماره کارت توسط کاربر، پیغام زیر به کاربر نمایش داده شود:

"مشتری گرامی، چنانچه از طریقی مانند برنامه کاربردی موبایلی، رمز پویای خود را دریافت نموده‌اید، نیازی به فشردن دکمه درخواست رمز پویا نمی‌باشد. در ادامه، رمز پویای خود را درقسمت رمز دوم کارت وارد نمایید."

نکته ۲: پس از فشردن دکمه‌ی «درخواست رمز پویا»، براساس پاسخ دریافت شده، یکی از عبارات زیر به کاربر نمایش داده شود:

۱. چنانچه بانک صادرکننده به سامانه هریم متصل نشده باشد:

"مشتری گرامی، بانک صادرکننده کارت شما در روزهای آتی به سامانه ارسال رمز پویا متصل خواهد شد. در حال حاضر، از رمز دوم ثابت کارت خود استفاده نمایید. لازم به ذکر است، رمز دوم ثابت کارت شما تا تاریخ ۹۸/۱۰/۱۵ معتبر خواهد بود"

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

۲. چنانچه بانک صادرکننده به سامانه هریم متصل شده باشد:

"مشتری گرامی، درخواست شما به بانک صادرکننده ارسال گردید. درصورت صحت اطلاعات وارد شده، رمز پویا از طریق پیامک به شماره تلفن همراه تاییده شده‌ی شما ارسال خواهد شد."

نکته ۳: در دکمه مربوط به «درخواست رمز پویا»، باید تایمر دو دقیقه‌ای با شمارش معکوس به کاربر نمایش داده شود. درصورتی که کاربر موفق به ورود «رمز پویا» در مدت زمان مذکور نشود، باید تا اتمام مهلت زمانی استفاده از صفحه پرداخت برنامه کاربردی موبایلی[۶] در باکس مربوط به «درخواست رمز پویا»، پیغام "دریافت مجدد رمز پویا" به کاربر به فاصله هر دو دقیقه یکبار، نمایش داده شود. حداکثر تعداد مرتبه مجاز در ارسال درخواست رمز پویا در مهلت زمانی برای صفحه پرداخت برنامه کاربردی موبایلی، پنج مرتبه است.

همچنین، درصورتی که کاربر موفق به ورود «رمز پویا» در مدت زمان مذکور نشود، پیغام زیر به کاربر نمایش داده شود:

"مشتری گرامی، در صورتی که از صحت اطلاعات وارد شده اطمینان دارید ولی هنوز رمز پویای خود را دریافت ننموده‌اید مجددا دکمه در خواست رمز پویا را بفشارید، در غیر اینصورت جهت رفع مشکل و تایید شماره تلفن همراه خود، به بانک صادر کننده مراجعه فرمایید."

نکته ۴: پس از پنج مرتبه درخواست رمز پویا توسط دارنده کارت، دارنده کارت به صفحه تراکنش ناموفق هدایت می‌گردد.

نکته ۵: تا پایان شمارش معکوس مهلت ۲ دقیقه‌ای، دکمه مربوط به درخواست رمز پویا می‌بایست غیرفعال باشد.

نکته ۶: فناوران مالی باید در برنامه کاربردی موبایلی خود، راهنمای مختصر به شرح زیر را درخصوص رمز پویا به کاربر نمایش دهند:

"راهنمای استفاده از رمز پویا"

رمز پویا، رمز یکبار مصرفی است که به جای رمز دوم کارت استفاده می‌شود.

مرحله اول- *براساس دستورالعمل بانک صادرکننده کارت خود، نسبت به فعال‌سازی رمز پویا اقدام نمایید.*

مرحله دوم-*رمز پویا را براساس روش اعلامی از طرف بانک صادرکننده کارت، به یکی از روش‌های زیر دریافت کنید.*

۱- دریافت از طریق برنامه کاربردی بانک، اینترنت‌بانک و یا موبایل‌بانک

---

[۶] مهلت انجام هر تراکنش توسط کاربر، در صفحه پرداخت برنامه کاربردی موبایلی پانزده دقیقه می‌باشد.

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

۲- دریافت از طریق کد USSD بانک صادرکننده کارت شما

۳- دریافت از طریق زدن دکمه‌ی "درخواست رمز پویا" در برنامه کاربردی موبایلی

***مرحله سوم**-پس از دریافت رمز به یکی از روش‌های فوق، رمز پویای دریافت شده را در محل تعیین شده برای "رمز دوم" وارد نمایید و سپس مابقی اطلاعات را تکمیل نمایید."*

نکته ۷: فناوران مالی باید ترتیبی اتخاذ نمایند تا درصورت درج شماره کارت مربوط به کارت‌های هدیه[۷]، پیغام زیر به کاربر نمایش داده شود.

"کاربر گرامی، کارت هدیه شما نیاز به دریافت رمز پویا(یک‌بارمصرف) ندارد. خواهشمند است از رمز دوم ثابت کارت هدیه خود استفاده فرمایید."

نکته ۸: در برنامه‌های کاربردی موبایلی، پس از انتخاب سرویسی که منجر به پرداخت می‌شود، فناوران مالی باید "راهنمای استفاده از رمز پویا" [۸]را به کاربر نمایش داده و سپس مراحل پرداخت مطابق با پیوست همین مستند، انجام شود.

نکته ۹: دریافت هرگونه اطلاعات به‌غیر از موارد بالا غیرمجاز است، مگر با مجوز شاپرک.

نکته ۱۰: کاربر تنها باید با سه کلید "درخواست رمز پویا"، "پرداخت" و "انصراف" هدایت لازم را دریافت نماید و حضور کلیدهای اضافی غیرمجاز می‌باشد.

تبصره: نمایش فهرست شماره کارت‌های استعلام شده از سامانه پیوند به صورت Truncated امکان‌پذیر است.

۵-۵-۲- رعایت الزامات امنیتی

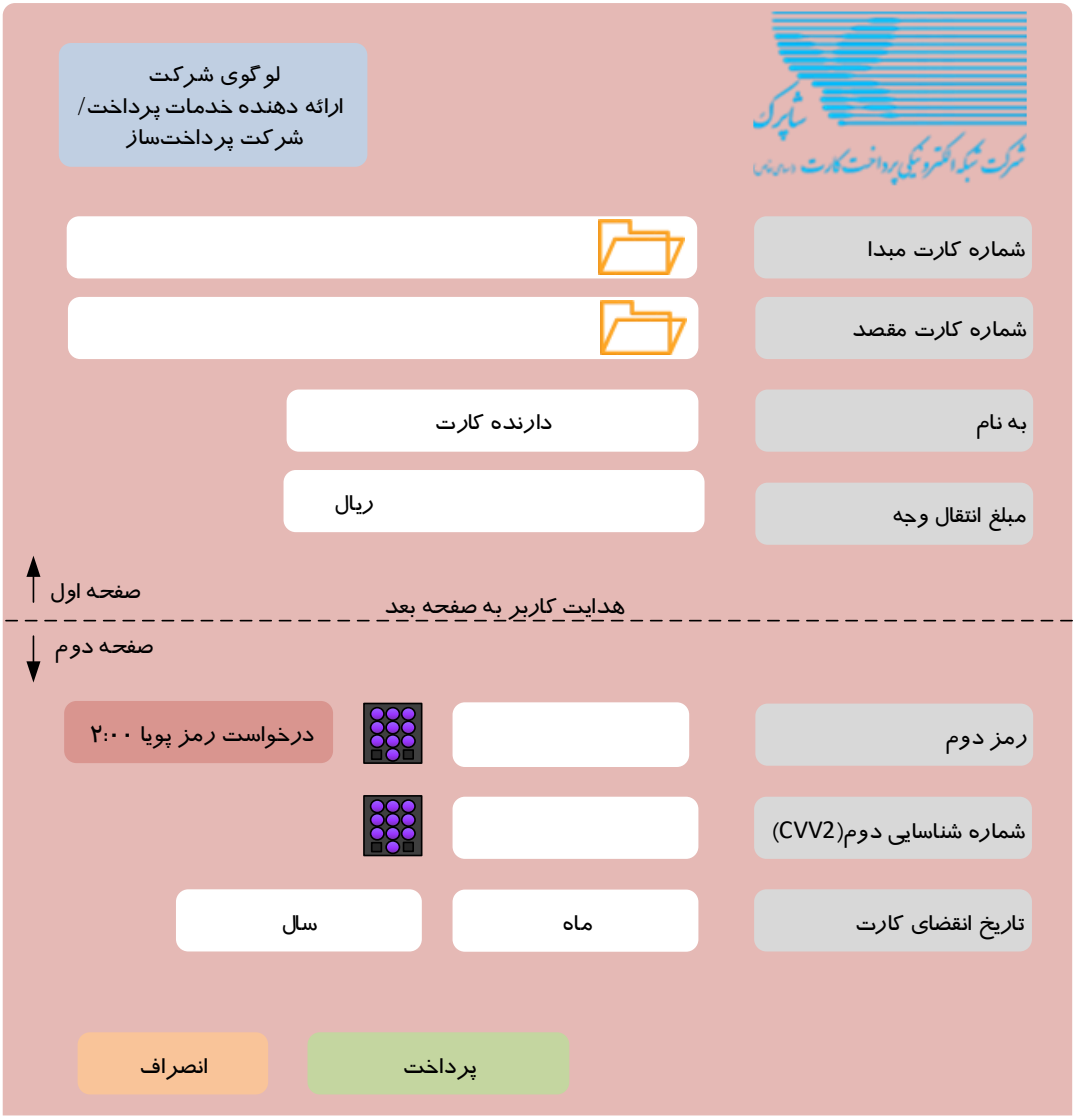
لازم به ذکر است رعایت کلیه الزامات امنیتی شاپرک در تمامی فرایندهای ارائه خدمت از طریق برنامه کاربردی موبایلی الزامی است.

[۷] کارت‌هایی که Product Code آن‌ها 2X و 3X باشد.

[۸] مطابق با متن مندرج در بخش راهنمای استفاده از رمز پویا در همین بند

هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.

۵-۶- پیوست- نمونه اقلام اطلاعاتی مندرج در برنامه‌های کاربردی موبایلی



هرگونه استفاده، چاپ، پخش و رونوشت برداری از این مستند بدون تایید کتبی شرکت شاپرک ممنوع می‌باشد.