شرکت شبکه الکترونیکی پرداخت کارت (سهامی خاص)

ضوابط و مقررات شاپرک

الزامات پرداخت‌های درون‌برنامه‌ای

کد مستند: SHP-STD-INAPPPURCHASE
ویرایش: 00-00
۱۳۹۷/۰۹/۱۱

شناسنامه مستند	
نگارنده	شبکه الکترونیکی پرداخت کارت-شاپرک
عنوان مستند	الزامات پرداخت‌های درون‌برنامه‌ای
کد مستند	SHP-STD-INAPPPURCHASE
شماره ویرایش	00-00
تاریخ تدوین/بازنگری	۱۳۹۷/۰۹/۱۱
تاریخ اجرا	متعاقبا اعلام می‌شود.
تاریخ مؤثر سند	متعاقبا اعلام می‌شود.
جامعه هدف	شرکت‌های ارائه دهنده خدمات پرداخت، شرکت‌های پرداخت‌یار، پذیرندگان تراکنش‌های درون‌برنامه‌ای
مراجع	_
مدارک ذیربط	الزامات امنیت اطلاعات شاپرک

کنترل نسخ مستندات

شماره ویرایش	موضوع بازنگری	تاریخ بازنگری	نگارنده
_	تاکنون بازنگری نشده است.	_	_

جدول ثبت تغییرات مدرک (مربوط به آخرین نسخه)

شماره تغییر	صفحه	محل تغییر	تغییرات اعمال شده	تاریخ بازنگری	نگارنده
_	_	_	_	_	_

فهرست مطالب

۱- مقدمه ۶
۲- اهداف ۶
۳- کاربران ۶
۴- تعاریف ۶
۴-۱-برنامه پرداخت ۶
۴-۲-API پرداخت ۶
۴-۳-SDK پرداخت ۷
۴-۴- ارائه دهنده API ۷
۴-۵- دریافت کننده API ۷
۴-۶- ارائه دهنده SDK ۷
۴-۷- دریافت کننده SDK ۷
۴-۸-پرداخت‌یار واجد شرایط دریافت API ۸
۴-۹- پذیرنده واجد شرایط دریافت API ۸
۴-۱۰- پرداخت‌یار واجد شرایط دریافت SDK ۸
۴-۱۱- پذیرنده واجد شرایط دریافت SDK ۸
۴-۱۲- پرداخت‌یار واجد شرایط ارائه SDK ۸
۴-۱۳- پرداخت موبایلی ۸
۴-۱۴- پرداخت درون برنامه‌ای ۹
۴-۱۵- نشان گذاری ۹
۴-۱۶- الزامات امنیت اطلاعات شاپرک ۹
۴-۱۷- درگاه پرداخت اینترنتی مجاز ۹
۴-۱۸- برنامه پرداخت مجاز ۹
۴-۱۹- سیستم میزبان ۹
۵- دامنه کاربرد ۹
۶-مدل‌های پرداخت موبایلی بدون حضور کارت با استفاده از برنامه‌های پرداخت ۱۰
۶-۱- روش‌های مبتنی بر عدم دریافت اطلاعات کارت توسط برنامه پرداخت ۱۰
۶-۱-۱- بهره‌گیری از یک روش نشان‌گذاری استاندارد ۱۰
۶-۱-۲- هدایت کاربر به درگاه پرداخت اینترنتی یکی از شرکت‌های ارائه دهنده خدمات پرداخت یا برنامه پرداخت مجاز ۱۰
۶-۲- روش‌های مبتنی بر دریافت اطلاعات کارت توسط برنامه پرداخت (یکپارچگی با درگاه پرداخت مجاز) ۱۰
۶-۲-۱- تولید برنامه پرداخت توسط شرکت ارائه دهنده خدمات پرداخت ۱۰
۶-۲-۲- استفاده از مکانیزم WEBVIEW ۱۱

۶-۲-۳- استفاده از **API** یا **SDK** مجاز ۱۱
۷- الزامات کلان پرداخت درون برنامه‌ای ۱۱
۸- الزامات امنیتی پرداخت درون‌برنامه‌ای ۱۱
۸-۱- الزامات امنیتی برنامه پرداخت تولید و ارائه شده توسط شرکت‌های ارائه دهنده خدمات پرداخت ۱۱
۸-۲- الزامات امنیتی ارائه **API** ۱۴
۸-۳- الزامات امنیتی ارائه **SDK** ۱۷
۸-۴- الزامات امنیتی دریافت **API** ۲۰
۸-۵- الزامات امنیتی استفاده از **WEBVIEW** ۲۲
۹- دسته‌بندی کسب و کاری ارائه خدمت پرداخت درون‌برنامه‌ای ۲۲
۹-۱- دسته‌بندی کسب و کاری شرکت‌های پرداخت‌یار، در پرداخت‌های درون‌برنامه‌ای ۲۲
۹-۲- دسته‌بندی کسب و کاری پذیرندگان عادی/پشتیبانی شده، در پرداخت‌های درون‌برنامه‌ای ۲۳
۱۰- بازه‌های زمانی انجام ممیزی از پرداخت‌یاران یا پذیرندگان عادی/پشتیبانی شده، در پرداخت‌های درون‌برنامه‌ای ۲۴

۱- مقدمه

پیشرفت‌های روزافزون فناوری و گسترش استفاده از ابزارهای موبایل موجب ظهورر و بروز کسب و کارهای جدید و به دنبال آن روش‌های نوین پرداخت الکترونیک شده است. در این راستا و به منظور توسعه کسب و کارهای مبتنی بر پرداخت‌های درون‌برنامه‌ای از یک سو و حصول اطمینان از حفظ امنیت اطلاعات کارت‌های بانکی از سوی دیگر، مستند حاضر تدوین گردیده است.

۲- اهداف

هدف از تدوین این سند، حصول اطمینان از حفظ محرمانگی اطلاعات کارت‌های بانکی و به حداقل رسیدن ریسک‌های امنیتی کلیه ذینفعان در شبکه پرداخت الکترونیک کشور، است.

۳- کاربران

کاربران این سند شرکت‌های ارائه دهنده خدمات پرداخت، شرکت‌های پرداخت‌یار و پذیرندگان تراکنش‌های درون‌برنامه‌ای درون‌برنامه‌ای می‌باشند.

۴- تعاریف

۴-۱- برنامه پرداخت

یک برنامه خاص نصب شده بر روی ابزار هوشمند(مانند و نه محدود به تلفن‌های همراه هوشمند) با قابلیت پرداخت است. این برنامه ممکن است توسط شرکت ارائه دهنده خدمات پرداخ، شرکت پرداخت‌یار و یا پذیرنده توسعه داده شود.

۴-۲- API[1] پرداخت

توابعی که امکان ارتباط دو سیستم با یکدیگر را فراهم نموده و ضمن فراخوانی از راه دور در متن "برنامه پرداخت" و با دریافت اطلاعات کارت، تراکنش پرداخت را انجام می‌دهند.

[1] Application Program Interface

۴-۳- SDK[۲] پرداخت

بسته نرم‌افزاری دارای قابلیت دریافت اطلاعات کارت و انجام تراکنش از راه دور، که به عنوان یک ماژول از پیش آماده شده، درون "برنامه پرداخت" قرار می‌گیرد.

۴-۴- ارائه دهنده API

شرکت ارائه دهنده خدمات پرداخت که "API پرداخت" را به شرکت‌های پرداخت‌یار واجد شرایط دریافت API و یا پذیرندگان واجد شرایط دریافت API، ارائه می‌نماید.

۴-۵- دریافت کننده API

شرکت پرداخت‌یار یا پذیرنده پرداخت‌های درون‌برنامه‌ای واجد شرایط تعریف شده در این مستند که می‌تواند تراکنش‌های خود را با استفاده از API ارائه شده توسط یکی از شرکت‌های ارائه دهنده خدمات پرداخت(با شرایط اعلام شده در این مستند) به شبکه پرداخت کشور ارسال کند.

۴-۶- ارائه دهنده SDK

شرکت ارائه دهنده خدمات پرداخت و یا شرکت پرداخت‌یار واجد شرایط ارائه SDK که می‌تواند با ارائه SDK به پذیرندگان عادی/پشتیبانی شده واجد شرایط دریافت SDK، تراکنش‌های ایشان به شبکه پرداخت کشور ارسال نماید.

۴-۷- دریافت کننده SDK

شرکت پرداخت‌یار یا پذیرنده پرداخت‌های درون‌برنامه‌ای واجد شرایط تعریف شده در این مستند که می‌تواند تراکنش‌های خود را با استفاده از SDK ارائه شده توسط یکی از شرکت‌های ارائه دهنده SDK که طبق الزامات این سند، مجاز به ارائه SDK می‌باشند، به شبکه پرداخت کشور ارسال کند.

[۲] Software Developers Kit

۴-۸- پرداخت‌یار واجد شرایط دریافت API

آن دسته از شرکت‌های پرداخت‌یار که مطابق با الزامات و مستندات شبکه پرداخت الکترونیکی کشور واجد شرایط پرداخت‌یاری شناخته شده و موفق به عقد موافقت‌نامه پرداخت‌یاری با شرکت شاپرک شده‌اند، و همچنین مطابق با جدول شماره(۱)، واجد شرایط دریافت API از یکی از ارائه دهندگان API می‌باشند.

۴-۹- پذیرنده واجد شرایط دریافت API

آن دسته از پذیرندگان شبکه پرداخت الکترونیکی کشور که وفق ضوابط و الزامات این شبکه، مجاز به دریافت خدمات پرداخت الکترونیکی هستند و براساس جدول شماره (۲)واجد شرایط دریافت API می‌باشند.

۴-۱۰- پرداخت‌یار واجد شرایط دریافت SDK

آن دسته از شرکت‌های پرداخت‌یار که مطابق با الزامات و مستندات شبکه پرداخت الکترونیکی کشور واجد شرایط پرداخت‌یاری شناخته شده و موفق به عقد موافقت‌نامه پرداخت‌یاری با شرکت شاپرک شده‌اند، و همچنین مطابق با جدول شماره(۱)، واجد شرایط دریافت SDK از یکی از ارائه دهندگان SDK می‌باشند.

۴-۱۱- پذیرنده واجد شرایط دریافت SDK

آن دسته از پذیرندگان یا پذیرندگان پشتیبانی شده شبکه پرداخت کشور که وفق ضوابط و الزامات شبکه پرداخت الکترونیکی کشور، مجاز به دریافت خدمات پرداخت الکترونیکی هستند و براساس جدول شماره (۲)، واجد شرایط دریافت SDK از ارائه دهنده SDK می‌باشند.

۴-۱۲- پرداخت‌یار واجد شرایط ارائه SDK

آن دسته از شرکت‌های پرداخت‌یار که مطابق با الزامات و مستندات شبکه پرداخت الکترونیکی کشور واجد شرایط پرداخت‌یاری شناخته شده و موفق به عقد موافقت‌نامه پرداخت‌یاری با شرکت شاپرک شده‌اند، و همچنین مطابق با جدول شماره(۱)، واجد شرایط ارائه SDK می‌باشند.

۴-۱۳- پرداخت موبایلی

به انجام خدمت پرداخت کارتی با استفاده از ابزار هوشمند(مانند و نه محدود به تلفن‌های همراه هوشمند) و به وسیله "برنامه پرداخت" گفته می‌شود.

۴-۱۴- پرداخت درون برنامه‌ای

خدمت پرداخت بدون حضور کارت (CNP) که توسط "برنامه پرداخت" ارائه شده است، به نحوی که اطلاعات لازم جهت انجام تراکنش در برنامه پرداخت، وارد می‌شود.

۴-۱۵- نشان گذاری[۳]

فرآیند جایگزین کردن شماره کارت (PAN) با مقداری تصادفی که به صورت برگشت‌پذیر و با هدف کاهش دامنه اجرای الزامات امنیت اطلاعات شاپرک انجام می‌شود.

۴-۱۶- الزامات امنیت اطلاعات شاپرک

الزامات کلان و کنترل‌های امنیتی ذکر شده در آخرین نسخه سند «الزامات امنیت اطلاعات شاپرک»، که با هدف مدیریت مخاطرات امنیتی مرتبط با اطلاعات کارت توسط شاپرک تدوین شده است.

۴-۱۷- درگاه پرداخت اینترنتی مجاز

درگاه پرداخت اینترنتی [۴](IPG) زیردامنه شاپرک که توسط شرکت های ارائه دهنده خدمات پرداخت، ارائه می‌شود.

۴-۱۸- برنامه پرداخت مجاز

"برنامه پرداختی" که مطابق با الزامات این سند، مجاز به ارائه خدمت "پرداخت درون برنامه‌ای" است.

۴-۱۹- سیستم میزبان

ابزار هوشمند(مانند و نه محدود به تلفن‌های همراه هوشمند) که "برنامه پرداخت" بر روی آن نصب شده است.

۵- دامنه کاربرد

دامنه کاربرد این سند، پرداخت‌های درون‌برنامه‌ای را که در آن اطلاعات لازم جهت انجام تراکنش، توسط کاربر در برنامه پرداخت وارد می‌شود، در برمی‌گیرد.

---

[۳] Tokenization

[۴] Internet Payment Gateway

۶- مدل‌های پرداخت موبایلی بدون حضور کارت با استفاده از برنامه‌های پرداخت

در این سند، چندین مدل پرداخت درون‌برنامه‌ای، بر اساس میزان دخالت اجزاء برنامه پرداخت، در هر یک از فرآیندهای پردازش، انتقال و ذخیره‌سازی اطلاعات کارت، در نظر گرفته شده است. مدل‌های مورد نظر به شرح زیر می‌باشند.

۶-۱- روش‌های مبتنی بر عدم دریافت اطلاعات کارت توسط برنامه پرداخت

در این روش، برنامه پرداخت در هیچ یک از سناریوهای ممکن جهت انجام تراکنش، اطلاعات کارت را از کاربر یا موجودیت دیگری دریافت نمی‌نماید. روش‌های مورد تایید شاپرک عبارتند از:

۶-۱-۱- بهره‌گیری از یک روش نشان‌گذاری استاندارد

۶-۱-۲- هدایت[۵] کاربر به درگاه پرداخت اینترنتی یکی از شرکت‌های ارائه دهنده خدمات پرداخت یا برنامه پرداخت مجاز

۶-۲- روش‌های مبتنی بر دریافت اطلاعات کارت توسط برنامه پرداخت (یکپارچگی با درگاه پرداخت مجاز)

در صورتی که برنامه پرداخت جهت انجام تراکنش، با یک درگاه پرداخت اینترنتی یا برنامه پرداخت دیگری که مورد تأیید شاپرک است، یکپارچه شده باشد، کاربر بدون اینکه از برنامه پرداخت خارج شود، اطلاعات کارت را وارد کرده و تراکنش انجام می‌شود. در این حالت، از دید کاربر، هیچ برنامه دیگری اطلاعات لازم برای انجام تراکنش را دریافت نمی‌کند.

روش‌های مجاز پیاده‌سازی یکپارچگی با درگاه پرداخت مجاز، به شرح زیر است:

۶-۲-۱- تولید برنامه پرداخت توسط شرکت ارائه دهنده خدمات پرداخت

در این حالت، برنامه پرداخت تحت مالکیت یکی از شرکت‌های ارائه دهنده خدمات پرداخت قرار داشته و توسعه این برنامه توسط شرکت ارائه دهنده خدمات پرداخت انجام می‌شود. برنامه پرداخت ضمن دریافت اطلاعات کارت، تراکنش را از طریق درگاه پرداخت اینترنتی مجاز تحت مالکیت شرکت ارائه دهنده خدمات پرداخت، به شبکه پرداخت ارسال می‌کند.

[۵] Redirect

۶-۲-۲- استفاده از مکانیزم WebView

صفحه پرداخت درگاه پرداخت اینترنتی مجاز، توسط برنامه پرداخت با استفاده از مکانیزم WebView درون برنامه پرداخت، باز شده و کاربر اطلاعات کارت را در آن وارد می‌کند. سپس تراکنش مستقیماً روی درگاه پرداخت اینترنتی مجاز انجام می‌شود.

۶-۲-۳- استفاده از API یا SDK مجاز

در این حالت برنامه پرداخت، از قابلیت‌های نرم‌افزاری ارائه شده توسط یکی از ارائه دهندگان API یا ارائه دهندگان SDK استفاده می‌کند. API یا SDK مسئول برقراری ارتباط برنامه پرداخت با درگاه پرداخت مجاز است. اطلاعات کارت توسط کاربر در برنامه پرداخت وارد شده و مستقیماً با استفاده از API یا SDK برای انجام تراکنش به درگاه پرداخت مجاز ارسال می‌شود.

۷- الزامات کلان پرداخت درون برنامه‌ای

الزامات مندرج در این سند، در دامنه کاربرد آن، در تکمیل سند «الزامات امنیت اطلاعات شاپرک» بوده و رعایت مفاد سند «الزامات امنیت اطلاعات شاپرک» به عنوان سند بالادستی، الزامی است.

۸- الزامات امنیتی پرداخت درون‌برنامه‌ای

در این بخش به بیان الزامات امنیتی هر یک از نقش‌های تعریف شده در این مستند پرداخته شده است. مخاطب الزامات باید مستندات و سوابق لازم جهت اثبات پیاده‌سازی هر الزام را ثبت و نگهداری نماید.

۸-۱- الزامات امنیتی برنامه پرداخت تولید و ارائه شده توسط شرکت‌های ارائه دهنده خدمات پرداخت

۸-۱-۱- توسعه امن: شرکت ارائه دهنده خدمات پرداخت باید چرخه مهندسی و توسعه امن نرم افزار[۶] را، مبتنی بر آخرین منابع و استانداردهای امنیت نرم‌افزارهای موبایلی، در توسعه برنامه پرداخت اجرا نموده و شواهد و سوابق مربوطه را مستند نماید.

۸-۱-۲- معماری امن: شرکت ارائه دهنده خدمات پرداخت باید کلیه مستندات معماری برنامه پرداخت، اجزای برنامه و کارکردهای آن و نیز شرح پروتکل‌های ارتباطی را به شاپرک ارائه و تأییدیه‌های امنیتی لازم را اخذ نماید.

[۶] Secure Software Development

۸-۱-۳- تبادل امن اطلاعات: شرکت ارائه دهنده خدمات پرداخت باید تضمین نماید که ارسال کلیه اطلاعات محرمانه و حساس (از جمله و نه محدود به اطلاعات کارت) از برنامه پرداخت تا درگاه پرداخت آن شرکت صرفاً با استفاده از رمزنگاری قوی[۷] و انتها به انتها[۸] انجام شود. استفاده از آخرین نسخه TLS و دیگر پروتکل‌های امنیت ارتباطات الزامی می‌باشد.

۸-۱-۴- تصدیق اصالت دارنده کارت: برنامه پرداخت شرکت ارائه دهنده خدمات پرداخت باید به یکی از روش‌های استاندارد مورد تایید شاپرک، دارنده کارت را به روشی امن و الزاماً با مشارکت بانک صادر کننده کارت، تصدیق اصالت نماید. روش‌های مورد تأیید شاپرک جهت پیاده‌سازی تصدیق اصالت دارنده کارت عبارتند از:

a. استفاده از عنصر امن[۹](SE) ابزار هوشمند(مانند و نه محدود به تلفن‌های همراه هوشمند) یا سیم‌کارت برای ذخیره‌سازی اطلاعات کارت مطابق با استانداردهای جهانی مرتبط
b. امکانات بیومتریک ابزار هوشمند(مانند و نه محدود به تلفن‌های همراه هوشمند) مانند و نه محدود به اثر انگشت دارنده کارت
c. استفاده از رمز یکبار مصرف
d. استفاده از برنامه تصدیق اصالت مجزا که توسط بانک صادرکننده ارائه شده است
e. استفاده از امکان محیط اجرای مورد اعتماد[۱۰](TEE) در سیستم عامل میزبان برنامه پرداخت برای ذخیره‌سازی اطلاعات کارت مطابق با استانداردهای جهانی مرتبط
f. پیاده‌سازی 3DSecure

جزئیات و شرایط مورد قبول برای هر یک از روش‌های تصدیق اصالت فوق توسط شاپرک ارائه خواهد شد.

۸-۱-۵- انتشار برنامه پرداخت به روش‌های مجاز: شرکت ارائه دهنده خدمات پرداخت باید برنامه پرداخت را صرفاً از وب‌سایت خود و نیز مجاری مجاز و شناخته شده و مورد اعتماد داخلی و خارجی جهت انتشار برنامه‌های موبایلی، منتشر کند و از انتشار آن در شبکه‌های اجتماعی و دیگر رسانه های متفرقه خودداری نماید.

۸-۱-۶- ارتباط با درگاه پرداخت مجاز: شرکت ارائه دهنده خدمات پرداخت باید ارتباط برنامه پرداخت را جهت انجام تراکنش، مستقیماً و بدون واسطه با درگاه پرداخت مجاز خود ایجاد نماید.

---

[۷] Strong Encryption

[۸] End to End

[۹] Secure Element

[۱۰] Trusted Execution Environment

۸-۱-۷- تصدیق اصالت برنامه پرداخت توسط درگاه پرداخت: برنامه پرداخت باید به صورت امن و منحصر به فرد، توسط درگاه پرداخت شرکت ارائه دهنده خدمات پرداخت تصدیق اصالت شود به نحوی که فقط برنامه مجاز تحت مالکیت شرکت ارائه دهنده خدمات پرداخت امکان اتصال به درگاه و انجام تراکنش را داشته باشد.

۸-۱-۸- تصدیق اصالت درگاه پرداخت توسط برنامه پرداخت: درگاه پرداخت باید به صورت امن و منحصر به فرد، توسط برنامه پرداخت تصدیق اصالت شود، به نحوی برنامه پرداخت فقط به درگاه پرداخت مجاز متصل شود و در صورت عدم احراز اصالت درگاه مجاز، برنامه پرداخت نباید موفق به شروع تراکنش شود.

۸-۱-۹- ارائه خدمات مجاز: شرکت ارائه دهنده خدمات پرداخت باید صرفاً خدماتی را توسط برنامه پرداخت (در حوزه‌های پرداخت و غیر پرداخت) ارائه نماید که ارائه آنها در برنامه پرداخت توسط شاپرک غیرمجاز شناخته نشده باشد.

۸-۱-۱۰- تداوم خدمت به برنامه پرداخت مجاز: شرکت ارائه دهنده خدمات پرداخت باید تمهیدات فنی لازم (مانند مدیریت ترافیک، محدود سازی تعداد درخواست‌ها از یک برنامه و غیره) را برای تداوم خدمت به همه نمونه‌های برنامه پرداخت مجاز و پیشگیری از حملات منجر به قطع خدمت (DoS)[۱۱] پیاده سازی نماید.

۸-۱-۱۱- ثبت لاگ: شرکت ارائه دهنده خدمات پرداخت باید تمام رویدادهای امنیتی از جمله و نه محدود به تمامی دسترسی‌های صورت گرفته به اطلاعات کارت، تمامی دسترسی‌های با سطح ادمین، دسترسی به لاگ‌های برنامه پرداخت، تلاش‌های دسترسی ناموفق به برنامه پرداخت، و غیره را با مشخص کردن شناسه کاربر، نوع رویداد، تاریخ و زمان رویداد، موفق و یا ناموفق بودن رویداد، منشا رویداد، منابع، داده‌ها و مولفه‌های تحت تاثیر رویداد، در سمت سرور ارائه دهنده خدمت، ثبت و نگهداری کند.

۸-۱-۱۲- امن سازی زیرساخت و اجزاء خدمت: شرکت ارائه دهنده خدمات پرداخت باید زیرساخت و کلیه اجزای ارائه خدمت برنامه پرداخت در سمت شرکت ارائه دهنده خدمات پرداخت را مطابق با استانداردهای معتبر، محکم‌سازی[۱۲] نماید.

۸-۱-۱۳- پیاده‌سازی امن برنامه پرداخت: شرکت ارائه دهنده خدمات پرداخت باید طراحی و توسعه برنامه پرداخت را مطابق با اصول برنامه‌سازی امن[۱۳] مربوط به زبان و تکنولوژی مورد استفاده انجام داده و شواهد مربوطه را مستند نماید.

۸-۱-۱۴- عدم استفاده از برنامه‌های عمومی و آماده: برنامه پرداخت و ماژول‌های آن نباید مبتنی بر برنامه های رایگان و در دسترس عموم پیاده‌سازی شود.

۸-۱-۱۵- حفاظت در برابر حملات مبتنی بر محتوا: شرکت ارائه دهنده خدمات پرداخت باید تمام محدودیت‌های لازم را در داخل کد برنامه پرداخت و نیز در طرف سرویس دهنده، برای حفاظت در برابر حملات مبتنی بر ارسال محتوای مخرب، اعمال نماید.

---

[۱۱] Denial of Service

[۱۲] Harden

[۱۳] Secure Coding

۸-۱-۱۶- حداقل مجوزهای دسترسی ممکن: توسعه برنامه پرداخت توسط شرکت ارائه دهنده خدمات پرداخت باید با رعایت اصل کمترین مجوزهای دسترسی ممکن انجام شود، به نحوی که برنامه پرداخت، صرفاً حداقل دسترسی‌های لازم برای کارکرد خود را در سیستم میزبان در اختیار داشته باشد.

۸-۱-۱۷- کنترل و ثبت تغییرات: کلیه تغییرات در نسخه یا امکانات برنامه پرداخت باید توسط شرکت ارائه دهنده خدمات پرداخت ثبت و مستند و قبل از اعمال، به شاپرک اعلام شود.

۸-۱-۱۸- حفاظت در برابر سرقت اطلاعات: شرکت ارائه دهنده خدمات پرداخت باید در پیاده‌سازی برنامه پرداخت، کلیه تمهیدات فنی بر اساس آخرین استانداردهای برنامه‌نویسی امن موبایل را برای پیشگیری از شنود و سرقت اطلاعات کارت و دیگر اطلاعات حساس توسط ماژول‌های غیر پرداختی برنامه پرداخت و دیگر برنامه‌های نصب شده در سیستم میزبان برنامه پرداخت، به کار گیرد.

۸-۱-۱۹- عدم ذخیره اطلاعات محرمانه در برنامه پرداخت: شرکت ارائه دهنده خدمات پرداخت باید از ذخیره اطلاعات کارت و دیگر اطلاعات محرمانه در داخل سیستم میزبان برنامه پرداخت اجتناب کند. ذخیره اطلاعات کارت صرفاً برای تصدیق اصالت دارنده کارت مطابق با الزامات این سند با استفاده از عنصر امن (SE) ابزار هوشمند(مانند و نه محدود به تلفن‌های همراه هوشمند) یا سیم کارت، مجاز است.

۸-۱-۲۰- عدم نقض حریم شخصی کاربر: شرکت ارائه دهنده خدمات پرداخت باید از استخراج اطلاعات شخصی کاربر توسط برنامه پرداخت یا ذخیره سازی اطلاعات شخصی (مانند و نه محدود به موقعیت مکانی کاربر، برنامه‌های نصب شده در سیستم میزبان، لیست مخاطبان) جز با مجوز صریح کاربر به ازای هر قلم از اطلاعات، خودداری نماید.

۸-۱-۲۱- حفاظت در برابر مهندسی معکوس: در پیاده‌سازی برنامه پرداخت باید کلیه تمهیدات فنی بر اساس آخرین استانداردهای برنامه‌نویسی امن موبایل برای پیشگیری از سوء استفاده از برنامه پرداخت با استفاده از مهندسی معکوس، به کار گرفته شود.

۸-۱-۲۲- آزمون امنیتی: شرکت ارائه دهنده خدمات پرداخت باید به صورت دوره‌ای و حداقل پیش از انتشار هر نسخه جدید برنامه پرداخت، آن را با ابزارها و روش‌های معتبر تست نفوذ، بر اساس نیازمندی‌های امنیتی و آسیب‌پذیری‌های معمول، تست کرده و نتایج را مستند و اعمال کند.

۸-۱-۲۳- مدیریت حوادث امنیتی: شرکت ارائه دهنده خدمات پرداخت باید هرگونه حادثه امنیتی ناشی از آسیب‌پذیری در برنامه پرداخت، سرور و دیگر اجزای ارائه خدمت پرداخت موبایلی را مطابق با روش اجرایی مدیریت حوادث امنیتی شاپرک، مدیریت نماید.

۸-۱-۲۴- آموزش تیم توسعه: شرکت ارائه دهنده خدمات پرداخت باید آموزش‌های مورد نیاز تیم توسعه برنامه پرداخت برای توسعه و برنامه نویسی امن موبایل را هر ساله اجرا و سوابق مربوطه را مستند نماید.

۸-۲- الزامات امنیتی ارائه API

۸-۲-۱- ارائه دهنده مجاز: ارائه API پرداخت صرفاً توسط شرکت ارائه دهنده خدمات پرداخت مجاز می‌باشد و شرکت‌های پرداخت‌یار یا پذیرندگان شبکه پرداخت کشور، مجاز به ارائه API پرداخت نمی‌باشند.

۸-۲-۲- ارائه API به شرکت‌های مجاز: شرکت ارائه دهنده صرفاً مجاز به ارائه API به شرکت‌هایی است که مطابق با الزامات این سند (رجوع به جداول شماره (۱) و (۲))، توسط شاپرک مجاز به دریافت API پرداخت شناخته شده باشند.

۸-۲-۳- پیاده‌سازی الزامات امنیت اطلاعات شاپرک: ارائه دهنده API باید کلیه الزامات امنیت اطلاعات شاپرک را پیاده‌سازی نماید، مگر در مواردی که کاربردناپذیری آنها در حوزه کسب و کاری ارائه API، به تأیید شاپرک برسد.

۸-۲-۴- معماری امن: شرکت ارائه دهنده باید کلیه مستندات معماری خدمت API، اجزا و کارکردهای آن و نیز شرح پروتکل‌های ارتباطی را به شاپرک ارائه و تأییدات امنیتی لازم را اخذ نماید.

۸-۲-۵- تصدیق اصالت[۱۴] فراخواننده: شرکت ارائه دهنده باید اصالت موجودیت فراخواننده API را در لایه شبکه و لایه برنامه کاربردی، به ازای هر تراکنش با استفاده از روش‌های استاندارد، امن و مورد تأیید شاپرک احراز نماید، به نحوی که فقط فراخواننده مجاز و شناخته شده، امکان پرداخت با API را داشته باشد.

۸-۲-۶- تصدیق اصالت دارنده کارت: ارائه دهنده API باید به یکی از روش‌های استاندارد مورد تایید شاپرک، دارنده کارت را به روشی امن و با مشارکت بانک صادر کننده کارت، تصدیق اصالت کند. روش‌های مورد تأیید جهت پیاده‌سازی تصدیق اصالت دارنده کارت عبارتند از:

a. استفاده از عنصر امن (SE) ابزار هوشمند(مانند و نه محدود به تلفن‌های همراه هوشمند) یا سیم کارت برای ذخیره سازی اطلاعات کارت مطابق با استانداردهای جهانی مرتبط
b. امکانات بیومتریک دستگاه موبایل مانند و نه محدود به اثر انگشت دارنده کارت
c. استفاده از رمز یکبار مصرف
d. استفاده از برنامه تصدیق اصالت مجزا که توسط بانک صادرکننده ارائه شده است.
e. استفاده از امکان محیط اجرای مورد اعتماد (TEE) در سیستم عامل میزبان برنامه پرداخت برای ذخیره‌سازی اطلاعات کارت مطابق با استانداردهای جهانی مرتبط
f. پیاده‌سازی 3DSecure

۸-۲-۷- ارائه API به پذیرندگان مجاز: شرکت ارائه دهنده خدمات پرداخت باید کلیه الزامات شاپرک جهت شناسایی پذیرنده مجاز را پیش از ارائه API و در طول ارائه خدمت API اجرا و در صورت تخطی پذیرنده از الزامات پذیرندگان شاپرک، ارائه خدمت را متوقف نماید.

[۱۴] Authentication

۸-۲-۸- اتصال بی‌واسطه به درگاه پرداخت مجاز: API ارائه شده باید به صورت مستقیم و بی‌واسطه، صرفاً به درگاه‌های پرداخت مورد تأیید شاپرک متصل شوند.

۸-۲-۹- تبادل امن اطلاعات: ارائه دهنده API باید تضمین کند که ارسال کلیه اطلاعات محرمانه و حساس (از جمله و نه محدود به اطلاعات کارت) از فراخواننده API تا درگاه پرداخت صرفاً با استفاده از رمزنگاری قوی و انتها به انتها انجام شود. استفاده از آخرین نسخه TLS الزامی می‌باشد.

۸-۲-۱۰- تداوم خدمت به برنامه پرداخت مجاز: شرکت PSP باید تمهیدات فنی لازم (مانند مدیریت ترافیک، محدود سازی تعداد درخواست‌ها و غیره) را برای تداوم خدمت به برنامه پرداخت مجاز و پیشگیری از حملات منجر به قطع خدمت پیاده سازی نماید.

۸-۲-۱۱- حفاظت در برابر حملات مبتنی بر محتوا: شرکت ارائه دهنده خدمات پرداخت باید تدابیر فنی برای حفاظت در برابر حملات ناشی از محتوای مخرب ارسالی توسط فراخواننده API را پیاده‌سازی و صرفاً محتوای دارای ساختار مجاز را قبول نماید.

۸-۲-۱۲- ثبت لاگ: تمام رویدادهای امنیتی، هویت کاربر، شناسه فراخواننده API و فعالیت‌های مهم API باید در طرف ارائه دهنده این خدمت (سرور) به صورت استاندارد و امن، ثبت و آرشیو شود.

۸-۲-۱۳- توسعه امن: شرکت ارائه دهنده باید چرخه مهندسی و توسعه امن نرم افزار مبتنی بر آخرین منابع و استانداردهای امنیت نرم افزار را در توسعه API پرداخت پیاده سازی نماید.

۸-۲-۱۴- پیاده سازی امن API: شرکت ارائه دهنده خدمات پرداخت باید اصول برنامه‌سازی امن[۱۵] را با توجه به زبان و تکنولوژی مورد استفاده در پیاده سازی API در طرف سرور به کار بندد.

۸-۲-۱۵- کنترل و ثبت تغییرات: کلیه تغییرات در نسخه API باید توسط شرکت ارائه دهنده خدمات پرداخت ثبت، مستند و قبل از اعمال تغییر، به شاپرک اعلام شود.

۸-۲-۱۶- آزمون امنیتی: شرکت باید به پیش از انتشار هر نسخه جدید API و حداقل هر سال یک بار، زیرساخت ارائه API را با ابزارها و روش‌های معتبر صنعت، بر اساس نیازمندی‌های امنیتی و آسیب‌پذیری‌های معمول، تست و نتایج را مستند و اعمال نماید.

۸-۲-۱۷- ممنوعیت دسترسی از راه دور: ارائه دسترسی از راه دور به سرور ارائه دهنده API تحت هر عنوانی غیر مجاز است.

[۱۵] Secure Coding

۸-۲-۱۸- تداوم کسب و کار: ارائه دهنده API باید طرح‌های تداوم کسب و کار را در حوزه خدمت API تدوین و اجرا نماید.

۸-۲-۱۹- مدیریت حوادث امنیتی: شرکت ارائه دهنده API باید هرگونه حادثه امنیتی ناشی از آسیب‌پذیری در برنامه پرداخت، سرور و دیگر اجزای ارائه خدمت پرداخت موبایلی را مطابق با روش اجرایی مدیریت حوادث امنیتی شاپرک، مدیریت نماید.

۸-۲-۲۰- آموزش تیم توسعه: شرکت ارائه دهنده API باید آموزش‌های مورد نیاز تیم توسعه برنامه پرداخت برای توسعه و برنامه‌نویسی امن موبایل را هر ساله اجرا و سوابق مربوطه را مستند نماید.

۸-۲-۲۱- امن سازی زیرساخت و اجزاء خدمت: شرکت ارائه دهنده API باید زیرساخت و کلیه اجزای ارائه خدمت API را در سمت سرویس دهنده مطابق با استانداردهای معتبر، محکم‌سازی نماید.

۸-۳- الزامات امنیتی ارائه SDK

در این بخش به ارائه الزامات امنیتی ارائه کننده SDK پرداخته شده است. ارائه SDK پرداخت، صرفاً توسط شرکت‌های ارائه دهنده خدمات پرداخت و شرکت‌های واجد شرایط جدول (۱) که به تأیید شاپرک رسیده‌اند، مجاز می‌باشد.

۸-۳-۱- ارائه کننده SDK باید کلیه الزامات امنیت اطلاعات شاپرک را پیاده‌سازی نماید، مگر در مواردی که کاربردناپذیری آن صرفاً در کسب و کار برنامه پرداخت، با ارائه دلائل و شواهد از سوی شرکت مربوطه، به تأیید شاپرک برسد.

۸-۳-۲- ممیزی الزامات امنیت: مسئولیت بازرسی و حصول اطمینان از پیاده‌سازی الزامات امنیت اطلاعات شاپرک و دیگر الزامات مربوطه در شرکت ارائه کننده SDK بر عهده شاپرک است.

۸-۳-۳- مسئولیت ارائه دهنده SDK: شرکت مجاز به ارائه SDK باید مسئولیت هرگونه سوء استفاده از اطلاعات کارت یا دیگر اطلاعات حساس مشتریان ناشی از نا امن بودن برنامه پرداخت را بر عهده بگیرد.

۸-۳-۴- انتشار برنامه پرداخت به روش‌های مجاز: شرکت ارائه دهنده SDK باید اطمینان حاصل نماید که برنامه پرداخت صرفاً در سرویس‌دهندگان شناخته شده و مورد اعتماد داخلی و خارجی، منتشر می‌گردد و از انتشار آن در شبکه‌های اجتماعی و دیگر رسانه‌های متفرقه خودداری گردد.

۸-۳-۵- تصدیق اصالت دارنده کارت: SDK باید به یکی از روش‌های استاندارد مورد تایید شاپرک، دارنده کارت را به روشی امن و با مشارکت بانک صادر کننده کارت، تصدیق اصالت نماید. روش‌های مورد تأیید جهت پیاده سازی تصدیق اصالت دارنده کارت عبارتند از:

- استفاده از عنصر امن (SE) ابزار هوشمند(مانند و نه محدود به تلفن‌های همراه هوشمند)یا سیم‌کارت برای ذخیره سازی اطلاعات کارت مطابق با استانداردهای جهانی مرتبط
- امکانات بیومتریک دستگاه موبایل مانند و نه محدود به اثر انگشت دارنده کارت
- استفاده از رمز یکبار مصرف

- استفاده از برنامه تصدیق اصالت مجزا که توسط بانک صادرکننده ارائه شده است
- استفاده از امکان محیط اجرای مورد اعتماد (TEE) در سیستم عامل میزبان برنامه پرداخت برای ذخیره سازی اطلاعات کارت مطابق با استانداردهای جهانی مرتبط
- پیاده سازی 3DSecure

جزئیات و شرایط مورد پذیرش برای هر یک از روش های تصدیق اصالت فوق توسط شاپرک ارائه خواهد شد.

۸-۳-۶- ارتباط با درگاه‌های پرداخت مجاز: ارائه کننده SDK باید به منظور انجام تراکنش، ارتباط مستقیم و بی‌واسطه صرفاً با درگاه پرداخت مورد تأیید شاپرک ایجاد نمایند.

۸-۳-۷- تصدیق اصالت درگاه پرداخت: SDK باید اصالت درگاه پرداخت مربوط را به ازای هر تراکنش به یکی از روش‌های تصدیق اصالت استاندارد و امن احراز نماید.

۸-۳-۸- تصدیق اصالت برنامه پرداخت: برنامه پرداخت باید به صورت امن و منحصر به فرد، توسط ارائه دهنده SDK تصدیق اصالت شود، به نحوی که صرفاً پذیرنده مجاز، امکان استفاده از خدمت SDK را داشته باشد.

۸-۳-۹- تبادل امن اطلاعات: ارتباط SDK با درگاه پرداخت الزاماً باید با رمزنگاری قوی و انتها به انتها انجام شود. استفاده از آخرین نسخه TLS الزامی می‌باشد.

۸-۳-۱۰- شناسایی پذیرنده مجاز: ارائه دهنده SDK باید از اهلیت و مجاز بودن پذیرندگان دریافت کننده SDK مطابق با الزامات پذیرندگان شاپرک، پیش و در طول ارائه خدمت اطمینان حاصل نماید.

۸-۳-۱۱- تداوم خدمت به برنامه پرداخت مجاز: ارائه دهنده SDK باید تمهیدات فنی لازم (مانند مدیریت ترافیک، محدود سازی تعداد درخواست‌ها و غیره) را برای تداوم خدمت به برنامه پرداخت مجاز و پیشگیری از حملات منجر به قطع خدمت پیاده سازی نماید.

۸-۳-۱۲- ثبت لاگ: تمام رویدادهای امنیتی از جمله و نه محدود به دسترسی‌های صورت گرفته به SDK، تمامی دسترسی‌های صورت گرفته به اطلاعات کارت، تمامی دسترسی‌های با سطح ادمین، دسترسی به لاگ‌های برنامه پرداخت، تلاش‌های دسترسی ناموفق به SDK، تمامی تغییرات در مکانیزم‌های شناسایی و تصدیق اصالت برنامه پرداخت و SDK و غیره را با مشخص کردن شناسه کاربر، نوع رویداد، تاریخ و زمان رویداد، موفق و یا ناموفق بودن رویداد، منشا رویداد، منابع، داده‌ها و مولفه‌های تحت تاثیر رویداد، در سمت سرور ارائه دهنده این خدمت، ثبت و نگهداری کند.

۸-۳-۱۳- پیاده‌سازی امن SDK: ارائه دهنده SDK باید طراحی و توسعه SDK را مطابق با اصول برنامه‌سازی امن[۱۶] مربوط به زبان و تکنولوژی مورد استفاده انجام دهد.

۸-۳-۱۴- عدم استفاده از برنامه‌های عمومی و آماده: SDK نباید مبتنی بر برنامه‌های رایگان و در دسترس عموم پیاده‌سازی شود.

۸-۳-۱۵- حفاظت در برابر حملات مبتنی بر محتوا: ارائه دهنده SDK باید تمام محدودیت‌های لازم را در کد SDK و نیز در طرف سرویس دهنده، برای حفاظت در برابر حملات مبتنی بر ارسال محتوای مخرب، اعمال نماید.

۸-۳-۱۶- کنترل دسترسی: توسعه SDK باید با رعایت اصل کمترین مجوزهای دسترسی مجاز انجام شود، به نحوی که برنامه پرداخت، صرفاً حداقل دسترسی‌های لازم برای کارکرد SDK را در سیستم میزبان در اختیار داشته باشد.

۸-۳-۱۷- کنترل و ثبت تغییرات: کلیه تغییرات در نسخه یا امکانات SDK باید توسط شرکت ارائه دهنده SDK ثبت و مستند و قبل از اعمال، به شاپرک اعلام شود.

۸-۳-۱۸- حفاظت در برابر سرقت اطلاعات: ارائه دهنده SDK در پیاده‌سازی SDK باید کلیه تمهیدات فنی بر اساس آخرین استانداردهای برنامه نویسی امن موبایل را برای پیشگیری از شنود و سرقت اطلاعات توسط برنامه پرداخت و دیگر برنامه‌های نصب شده در سیستم میزبان برنامه پرداخت را به کار گیرد.

۸-۳-۱۹- عدم ذخیره اطلاعات محرمانه در برنامه پرداخت: ارائه دهنده SDK باید از ذخیره اطلاعات کارت و دیگر اطلاعات محرمانه در داخل سیستم میزبان برنامه پرداخت اجتناب کند. ذخیره اطلاعات کارت صرفاً برای تصدیق اصالت دارنده کارت مطابق با الزامات این سند با استفاده از عنصر امن (SE) ابزار هوشمند(مانند و نه محدود به تلفن‌های همراه هوشمند)یا سیم کارت، مجاز است.

۸-۳-۲۰- عدم نقض حریم شخصی کاربر: شرکت ارائه دهنده SDK باید از استخراج اطلاعات شخصی کاربر توسط SDK یا ذخیره‌سازی اطلاعات شخصی (مانند و نه محدود به موقعیت مکانی کاربر، برنامه های نصب شده در سیستم میزبان، لیست مخاطبان) جز با مجوز صریح کاربر به ازای هر قلم از اطلاعات، خودداری نماید.

۸-۳-۲۱- حفاظت در برابر مهندسی معکوس: در پیاده‌سازی SDK کلیه تمهیدات فنی بر اساس آخرین استانداردهای برنامه‌نویسی موبایل برای پیشگیری از سوء استفاده از SDK بر اساس مهندسی معکوس باید به کار گرفته شود.

۸-۳-۲۲- آزمون امنیتی: شرکت ارائه دهنده SDK باید به صورت دوره‌ای و حداقل پیش از انتشار هر نسخه جدید SDK، آن را با ابزارها و روش‌های معتبر و مورد تایید صنعت، بر اساس نیازمندی‌های امنیتی و آسیب پذیری‌های معمول، تست کرده و نتایج را مستند و اعمال کند.

[۱۶] Secure Coding

۸-۳-۲۳- تحویل امن SDK: ارائه دهنده SDK باید یک فرآیند مستند شده و امن برای ارائه آخرین نسخه عملیاتی SDK به شرکت توسعه دهنده برنامه پرداخت، طراحی و اجرا کند.

۸-۳-۲۴- ممنوعیت دسترسی از راه دور: ارائه مجوز دسترسی از راه دور به سرور SDK تحت هر عنوانی غیرمجاز است.

۸-۳-۲۵- آموزش تیم توسعه: ارائه دهنده SDK باید آموزش‌های موردنیاز تیم توسعه برنامه پرداخت برای توسعه و برنامه نویسی امن موبایل را هر ساله اجرا و سوابق مربوطه را مستند نماید.

۸-۳-۲۶- امن‌سازی زیرساخت و اجزاء خدمت: ارائه دهنده SDK باید زیرساخت و کلیه اجزای ارائه خدمت SDK در سمت سرویس دهنده را مطابق با استانداردهای معتبر، محکم‌سازی نماید.

۸-۴- الزامات امنیتی دریافت API

در این بخش به ارائه الزامات امنیتی دریافت کننده API پرداخته شده است. صرفاً شرکت‌های پرداخت‌یار و پذیرندگان واجد شرایط جداول (۱) و (۲) که به تأیید شاپرک رسیده‌اند مجاز به دریافت API پرداخت از شرکت‌های ارائه دهنده خدمات پرداخت می‌باشند.

۸-۴-۱- دریافت کننده API باید کلیه الزامات امنیت اطلاعات شاپرک را پیاده سازی نماید، مگر در مواردی که کاربردناپذیری آن صرفاً در کسب و کار برنامه پرداخت، با ارائه دلائل و شواهد از سوی شرکت مربوطه، به تأیید شاپرک برسد.

۸-۴-۲- ممیزی الزامات امنیت: مسئولیت بازرسی و حصول اطمینان از پیاده‌سازی الزامات امنیت اطلاعات شاپرک و دیگر الزامات مربوطه در شرکت دریافت کننده API بر عهده شاپرک است.

۸-۴-۳- تصدیق اصالت دارنده کارت: فراخواننده API باید به یکی از روش‌های استاندارد مورد تایید شاپرک، دارنده کارت را به روشی امن و با مشارکت بانک صادر کننده کارت، تصدیق اصالت کند. روش‌های مورد تأیید جهت پیاده سازی تصدیق اصالت دارنده کارت عبارتند از:

- استفاده از عنصر امن (SE) تجهیز موبایل یا سیم کارت برای ذخیره سازی اطلاعات کارت مطابق با استانداردهای جهانی مرتبط
- امکانات بیومتریک دستگاه موبایل مانند و نه محدود به اثر انگشت دارنده کارت
- استفاده از رمز یکبار مصرف
- استفاده از برنامه تصدیق اصالت مجزا که توسط بانک صادرکننده ارائه شده است.
- استفاده از امکان محیط اجرای مورد اعتماد (TEE) در سیستم عامل میزبان برنامه پرداخت برای ذخیره سازی اطلاعات کارت مطابق با استانداردهای جهانی مرتبط
- پیاده سازی 3DSecure

جزئیات و شرایط مورد پذیرش برای هر یک از روش های تصدیق اصالت فوق توسط شاپرک ارائه خواهد شد.

۸-۴-۴- ارتباط با درگاه‌های پرداخت مجاز: دریافت کننده API باید به منظور انجام تراکنش، ارتباط مستقیم و بی‌واسطه صرفاً با درگاه پرداخت مورد تأیید شاپرک ایجاد نمایند.

۸-۴-۵- تصدیق اصالت ارائه دهنده API: فراخواننده API باید به ازای هر فراخوانی، اصالت ارائه دهنده API را به یکی از روش‌های تصدیق اصالت استاندارد و امن احراز نماید.

۸-۴-۶- تبادل امن اطلاعات: ارتباط دریافت کننده API با درگاه پرداخت الزاماً باید با رمزنگاری قوی و انتها به انتها انجام شود. استفاده از آخرین نسخه TLS الزامی می‌باشد.

۸-۴-۷- پذیرنده مجاز: دریافت کننده API باید مقررات و الزامات مربوط به پذیرندگان مجاز شاپرک را رعایت نماید.

۸-۴-۸- ثبت لاگ: تمام رویدادهای امنیتی از جمله و نه محدود به درخواست‌های ارسال شده به API، تمامی دسترسی‌های صورت گرفته به اطلاعات کارت، تمامی دسترسی‌های با سطح ادمین، دسترسی به لاگ‌های برنامه پرداخت، تلاش‌های دسترسی ناموفق به API، تمامی تغییرات در مکانیزم‌های شناسایی و تصدیق اصالت برنامه پرداخت و API و غیره را با مشخص کردن شناسه کاربر، نوع رویداد، تاریخ و زمان رویداد، موفق و یا ناموفق بودن رویداد، منشا رویداد، منابع، داده‌ها و مولفه‌های تحت تاثیر رویداد، در سمت سرور ارائه دهنده این خدمت، ثبت و نگهداری کند.

۸-۴-۹- حفاظت در برابر حملات مبتنی بر محتوا: دریافت کننده API باید تمام محدودیت‌های لازم را در طرف فراخواننده، برای حفاظت در برابر حملات مبتنی بر ارسال محتوای مخرب، اعمال نماید.

۸-۴-۱۰- پیاده‌سازی امن فراخوانی‌های API: ارائه دهنده و دریافت کننده API باید مطابق با اصول برنامه سازی امن[۱۷] مربوط به زبان و تکنولوژی مورد استفاده، فراخوانی‌های مورد نیاز را انجام دهند.

۸-۴-۱۱- عدم استفاده از برنامه‌های عمومی و آماده: پیاده‌سازی استفاده از API نباید مبتنی بر برنامه‌های رایگان و در دسترس عموم انجام شود.

۸-۴-۱۲- کنترل دسترسی: پیاده‌سازی راهکار API باید با رعایت اصل کمترین مجوزهای دسترسی مجاز انجام شود، به نحوی که برنامه پرداخت، صرفاً حداقل دسترسی‌های لازم برای دسترسی به API را در سیستم میزبان در اختیار داشته باشد.

۸-۴-۱۳- حفاظت در برابر سرقت اطلاعات: دریافت کننده API باید کلیه تمهیدات فنی بر اساس آخرین استانداردهای برنامه نویسی امن را برای پیشگیری از شنود و سرقت اطلاعات در طرف فراخواننده به کار گیرد.

[۱۷] Secure Coding

۸-۴-۱۴- عدم ذخیره اطلاعات محرمانه: دریافت کننده API باید از ذخیره اطلاعات کارت و دیگر اطلاعات محرمانه در طرف فراخواننده اجتناب کند. ذخیره اطلاعات کارت صرفاً برای تصدیق اصالت دارنده کارت مطابق با الزامات این سند با استفاده از عنصر امن (SE) ابزار هوشمند(مانند و نه محدود به تلفن‌های همراه هوشمند)یا سیم کارت، مجاز است.

۸-۴-۱۵- آزمون امنیتی: شرکت دریافت کننده API باید به صورت دوره‌ای و حداقل پیش از انتشار هر نسخه جدید راهکار API، کل راهکار را با ابزارها و روش‌های معتبر و مورد تایید صنعت، بر اساس نیازمندی‌های امنیتی و آسیب‌پذیری‌های معمول، تست کرده و نتایج را مستند و اعمال کند.

۸-۴-۱۶- ممنوعیت دسترسی از راه دور: ارائه دسترسی از راه دور به سرور برنامه پرداخت تحت هر عنوانی غیرمجاز است.

۸-۵- الزامات امنیتی استفاده از WebView

الزامات استفاده از WebView ، مانند الزامات دریافت API می‌باشد.

۹- دسته‌بندی کسب و کاری ارائه خدمت پرداخت درون‌برنامه‌ای

متقاضیان ارائه خدمت پرداخت درون‌برنامه‌ای جهت ارائه این خدمت، علاوه بر الزامات ذکر شده در بندهای فوق، بایستی واجد شرایط مندرج در جداول زیر نیز باشند:

۹-۱- دسته‌بندی کسب و کاری شرکت‌های پرداخت‌یار، در پرداخت‌های درون‌برنامه‌ای

نوع پذیرنده	سطح	تعداد/جمع مبلغ تراکنش	دریافت API	ارائه SDK	دریافت SDK	Redirect
پرداخت‌یار	یک	بیش از ۶ میلیون تراکنش سالانه یا جمع مبلغی بیش از ۱،۰۰۰،۰۰۰،۰۰۰،۰۰۰ ریال (از طریق ابزار پذیرش اینترنتی)	☑	☑	☑	☑
پرداخت‌یار	دو	۲ تا ۶ میلیون تراکنش در سال یا جمع مبلغی از ۶۰۰،۰۰۰،۰۰۰،۰۰۰ تا ۱،۰۰۰،۰۰۰،۰۰۰،۰۰۰ ریال (از طریق ابزار پذیرش اینترنتی)	☒	☒	☑	☑

نوع پذیرنده	سطح	تعداد/جمع مبلغ تراکنش	دریافت API	ارائه SDK	دریافت SDK	Redirect
پرداخت‌یار	سه	کمتر از ۲ میلیون تراکنش سالانه یا جمع مبلغی کمتر از ۶۰۰،۰۰۰،۰۰۰،۰۰۰ ریال (از طریق ابزار پذیرش اینترنتی)	☒	☒	☒	☑

جدول ۱- دسته‌بندی کسب و کاری شرکت‌های پرداخت‌یار، در پرداخت‌های درون‌برنامه‌ای

۹-۲- دسته‌بندی کسب و کاری پذیرندگان عادی/پشتیبانی شده، در پرداخت‌های درون‌برنامه‌ای

نوع پذیرنده	سطح	تعداد/جمع مبلغ تراکنش	دریافت API	دریافت SDK	Redirect
پذیرنده عادی/ پشتیبانی شده	یک	بیش از ۶ میلیون تراکنش سالانه یا جمع مبلغی بیش از ۱،۰۰۰،۰۰۰،۰۰۰،۰۰۰ ریال (از طریق ابزار پذیرش اینترنتی)	☑	☑	☑
پذیرنده عادی/ پشتیبانی شده	دو	۲ تا ۶ میلیون تراکنش در سال یا جمع مبلغی از ۶۰۰،۰۰۰،۰۰۰،۰۰۰ تا ۱،۰۰۰،۰۰۰،۰۰۰،۰۰۰ ریال (از طریق ابزار پذیرش اینترنتی)	☒	☑	☑
پذیرنده عادی/ پشتیبانی شده	سه	کمتر از ۲ میلیون تراکنش سالانه یا جمع مبلغی کمتر از ۶۰۰،۰۰۰،۰۰۰،۰۰۰ ریال (از طریق ابزار پذیرش اینترنتی)	☒	☒	☑

جدول ۲- دسته‌بندی کسب و کاری پذیرندگان عادی/پشتیبانی شده، در پرداخت‌های درون‌برنامه‌ای

۱۰- بازه‌های زمانی انجام ممیزی از پرداخت‌یاران یا پذیرندگان عادی/پشتیبانی شـــده، در پرداخت‌های درون‌برنامه‌ای

نظارت بر شرکت‌های دامنه کاربرد این سند، براساس جدول زیر انجام می‌شود، با این وجود مسئولیت هرگونه سـوء اسـتفاده از اطلاعات کارت یا دیگر اطلاعات حساس مشتریان ناشی از نا امن بودن برنامه پرداخت، بر عهـده ارائـه دهنـده SDK/API می‌باشـد و این شرکت باید تمهیدات فنی و اجرایی و تضامین لازم را جهت پیشگیری و جبران خسارت ناشی از نا امـن بـودن برنامـه پرداخـت، اعمال نماید.

سطح	ناظر	بازه زمانی انجام ممیزی از پرداخت‌یار/پذیرنده
یک	شرکت ارائه دهنده خدمات پرداخت	هر سه ماه یکبار
	شرکت شاپرک	حداقل هر ۶ ماه یکبار
دو	شرکت ارائه دهنده خدمات پرداخت	هر سه ماه یکبار
سه	شرکت ارائه دهنده خدمات پرداخت	انجام ممیزی مطابق با روال معمول و عادی
	شرکت شاپرک	انجام ممیزی مطابق با روال معمول و عادی

جدول ۳- بازه‌های زمانی انجام ممیزی از پرداخت‌یاران یا پذیرندگان عادی/پشتیبانی شده، در پرداخت‌های درون‌برنامه‌ای