شرکت شبکه الکترونیکی پرداخت کارت (سهامی خاص)

ضوابط و مقررات شاپرک

الزامات ابزارهای پذیرش

کد مستند: SHP_RGL_PAYMENTDEVICE

ویرایش: 00-06

۱۴۰۲/۰۴/۲۴

شناسنامه مستند	
نگارنده	شبکه الکترونیکی پرداخت کارت-شاپرک
عنوان مستند	الزامات ابزارهای پذیرش
کد مستند	SHP_RGL_PAYMENTDEVICE
شماره ویرایش	06-00
تاریخ تدوین/بازنگری	۱۴۰۲/۰۴/۲۴
تاریخ اجرا	بلافاصله پس از ابلاغ
تاریخ مؤثر سند	بلافاصله پس از ابلاغ
طبقه‌بندی محرمانگی	انتشار محدود
جامعه هدف	شرکت‌های ارائه دهنده خدمات پرداخت
مراجع	مجموعه الزامات انجمن PCI
مدارک ذیربط	الزامات امنیت اطلاعات شاپرک
	مقررات استفاده از نام و نشان تجاری شاپرک
	مقررات صدور رسیدهای الکترونیکی در پرداخت‌های الکترونیکی مبتنی بر کارت
	مقررات صدور برگه رسید پایانه‌های فروش
	یکسان‌سازی منوی پایانه‌های فروش
	دستورالعمل درخواست اعمال تغییرات در خدمات شرکت‌های ارائه‌دهنده خدمات پرداخت
	الزامات تولید فایل درخواست جهت صدور گواهی امنیتی
	بخشنامه بانک مرکزی ج.ا.ا به شماره ۹۷/۴۳۴۷۷۵ مورخ ۱۳۹۷/۱۲/۰۶
	بخشنامه بانک مرکزی ج.ا.ا به شماره ۹۶/۳۵۱۱۹۵ مورخ ۱۳۹۶/۱۱/۰۲
	بخشنامه بانک مرکزی ج.ا.ا به شماره ۹۶/۳۶۰۵۲۱ مورخ ۱۳۹۶/۱۱/۰۹

کنترل نسخ مستندات

شماره ویرایش	موضوع بازنگری	تاریخ بازنگری	نگارنده
02-00	به دلیل پراکندگی تغییرات به ویرایش دوم سند رجوع شود.	۱۳۹۵/۰۵/۲۳	شاپرک
03-00	بازنگری کلی	۱۳۹۸/۰۶/۰۲	شاپرک
03-02	- بروزرسانی کنترل «اطلاعات مجاز قابل دریافت در صفحه پرداخت» - افزودن پیوست (۱) با عنوان «نمونه اقلام اطلاعاتی مندرج در صفحات پرداخت اینترنتی و موبایلی»	۱۳۹۸/۰۸/۲۶	شاپرک
04-00	به دلیل پراکندگی تغییرات به ویرایش چهارم سند رجوع شود.	۱۳۹۹/۰۸/۲۰	شاپرک
05-00	- افزودن بند ۵-۲-۲ - تکمیل بند ۵-۲-۱-۱۶	۱۴۰۰/۰۶/۱۰	شاپرک
06-00	بازنگری کلی	۱۴۰۲/۰۴/۲۴	شاپرک

جدول ثبت تغییرات مدرک (مربوط به آخرین نسخه)

شماره تغییر	صفحه	محل تغییر	تغییرات اعمال شده	تاریخ بازنگری	نگارنده
-	-	-	بازنگری کلی	۱۴۰۲/۰۴/۲۴	شاپرک

فهرست مطالب

۱- مقدمه

به منظور یکپارچه‌سازی قواعد استفاده از ابزارهای پذیرش، لازم است حداقل الزامات کلان این ابزارها به منظور به کارگیری در شبکه پرداخت کشور تدوین شده و به کار گرفته شود. در این سند، ابزارهای پذیرش به دو گروه ابزار پذیرش با حضور کارت (شامل دستگاه کارت‌خوان، M-POS، دستگاه Pin Pad و پایانه فروش خودکار) و ابزار پذیرش بدون حضور کارت (درگاه پرداخت اینترنتی و موبایلی) دسته‌بندی شده و الزامات مرتبط با هر دسته به صورت مجزا ارائه شده است.

۲- اهداف

مستند حاضر، به منظور تعیین الزامات ابزارهای پذیرش ارائه شده است.

۳- کاربران

کاربران این سند، شرکت‌های ارائه دهنده خدمات پرداخت می‌باشند.

۴- تعاریف

۴-۱- بانک

کلیه بانک‌ها و موسسات مالی و اعتباری عضو شتاب.

۴-۲- دارنده کارت

شخص حقیقی یا حقوقی است که کارت بانکی توسط بانک به نام وی صادر شده است.

۴-۳- پذیرنده

شخص حقیقی یا حقوقی است که با پذیرش کارت بانکی و با استفاده از ابزار پذیرش نسبت به عرضه کالا و یا ارائه خدمات به دارندگان کارت اقدام می‌کند.

۴-۴- ابزار پذیرش

عبارت است از سخت‌افزار و نرم‌افزاری که امکان انجام تراکنش را برای دارنده کارت فراهم می‌سازد.

۴-۵- ابزار پذیرش با حضور کارت

عبارت است از انواع ابزار پذیرش که انجام تراکنش از طریق آن نیازمند استفاده از کارت(اعم از فیزیکی یا مجازی) به صورت حضوری و در محل پذیرنده می‌باشد. این ابزار شامل انواع پایانه‌های فروش[۱] با سیستم‌عامل‌های مختلف، کیوسک پرداخت و ... است.

۴-۶- ابزار پذیرش با حضور کارت[۲] متصل

هر ابزار پذیرش با حضور کارت، که به سوئیچ شرکت ارائه‌دهنده خدمات پرداخت متصل بوده و از طریق سوئیچ شاپرک قادر به انجام تراکنش می‌باشد.

---

[۱] POS

[۲] Card Present

۴-۷- ابزار پذیرش با حضور کارت غیرمتصل

هر ابزار پذیرش با حضور کارت، که شماره سریال آن در موجودی انبار شرکت ارائه‌دهنده خدمات پرداخت لحاظ شده است و به هیچ پذیرنده و ترمینالی تخصیص داده نشده است.

۴-۸- ابزار پذیرش فعال سیستمی

ابزار پذیرشی است که وضعیت آن در سوئیچ شاپرک فعال تعریف شده است.

۴-۹- ابزار پذیرش غیرفعال سیستمی

ابزار پذیرشی است که وضعیت آن در سوئیچ شاپرک غیرفعال تعریف شده است.

۴-۱۰- PCI-SSC[۳]

انجمن استانداردهای امنیتی صنعت پرداخت کارتی، که متولی تدوین، اعمال و ممیزی استانداردهای امنیتی کارت از جمله و نه محدود به PCI-DSS، PCI-PTS و PA-DSS است.

۴-۱۱- برنامه کاربردی پرداخت

منظور از برنامه کاربردی پرداخت، برنامه اصلی پرداخت ابزار پذیرش می‌باشد.

۴-۱۲- برنامه کاربردی جانبی

منظور از برنامه کاربردی جانبی، برنامه کاربردی می‌باشد که توسط شرکت ارائه دهنده خدمات پرداخت یا سایر شرکت‌های ثالث همکار، برای کاربردها و کسب و کارهای خاص منظوره، توسعه داده شده است.

۴-۱۳- نقطه تعامل (POI[۴])

به نقطه اولیه‌ای که داده‌ها از کارت خوانده می‌شوند، اطلاق می‌گردد. در واقع یک محصول پذیرش تراکنش الکترونیکی است که شامل سخت‌افزار و نرم‌افزار بوده و در ابزار پذیرش میزبانی می‌شوند تا دارنده کارت قادر به انجام تراکنش کارتی باشد. دستگاه‌های POI PTS مورد تأیید PCI، دستگاه‌هایی هستند که گواهینامه را از طریق یک آزمایشگاه تأیید شده PCI دریافت کرده‌اند.

[۳] Payment Card Industry Security Standards Council

[۴] Point Of Interaction

۵- شرح

۵-۱- الزامات کلان ابزارهای پذیرش

۵-۱-۱- تمامی ابزارهای پذیرش با حضور کارت شرکت ارائه‌دهنده خدمات پرداخت که فعال سیستمی می‌باشند، باید در مستندی تحت عنوان شناسنامه آماری ابزارهای پذیرش متصل، مطابق با الزام مندرج در بند (۵-۲-۱-۱۰) ثبت شوند و به تأیید مدیرعامل شرکت ارائه‌دهنده خدمات پرداخت برسد.

۵-۱-۲- تمامی ابزارهای پذیرش با حضور کارت شرکت ارائه‌دهنده خدمات پرداخت که غیرفعال سیستمی بوده و در انبار شرکت ارائه‌دهنده خدمات پرداخت موجود می‌باشند، باید در مستندی تحت عنوان شناسنامه آماری ابزارهای پذیرش غیرمتصل، مطابق با الزام مندرج در بند (۵-۲-۱-۱۰) ثبت شوند و به تأیید مدیرعامل شرکت ارائه‌دهنده خدمات پرداخت برسد.

۵-۱-۳- مسئولیت صحت‌سنجی اسناد و مدارک تمامی پذیرندگان بر عهده شرکت ارائه دهنده خدمات پرداخت بوده و باید مدارک دریافتی از پذیرندگان نزد شرکت ارائه دهنده خدمات پرداخت نگهداری شود.

۵-۱-۴- شرکت ارائه‌دهنده خدمات پرداخت باید هرگونه تغییر در منو یا اطلاعات ابزارهای پذیرش خود (ابزار پذیرش با حضور کارت و ابزار پذیرش بدون حضور کارت) را قبل از اعمال در محیط عملیاتی به شرکت شاپرک اطلاع دهد. نحوه اطلاع‌رسانی به شرکت شاپرک باید مطابق با سند «درخواست اعمال تغییرات در خدمات شرکت‌های ارائه‌دهنده خدمات پرداخت» انجام گیرد.

۵-۱-۵- شرکت ارائه‌دهنده خدمات پرداخت پیش از اقدام به تغییر نام، لوگو یا هر مشخصه دیگر که قبل از آن برای معرفی خود استفاده نموده، می‌بایست ضمن اطلاع‌رسانی به شرکت شاپرک، تأیید بانک مرکزی در این خصوص را اخذ نموده باشد.

۵-۱-۶- قابلیت E2EE[۵] در کلیه تراکنش‌های بدون حضور کارت مبتنی بر بستر اینترنت، باید پیاده‌سازی شده باشد.

۵-۱-۷- انجام تراکنش‌های بدون حضور کارت در کلیه کانال‌های فاقد رمزنگاری مبدأ تا مقصد توسط کلیدهای معتبر بانکی، صرفاً با پذیرش تمامی مسئولیت‌های مترتبه توسط پذیرنده و بانک صادرکننده کارت امکان‌پذیر است.

۵-۱-۸- هرگونه توسعه و ارائه خدمت جدید در کانال‌های فاقد رمزنگاری مبدأ تا مقصد اکیداً ممنوع می‌باشد.

۵-۱-۹- سرویس مانده‌گیری از درگاه‌های پرداخت بدون حضور کارت تنها از بسترهای دارای رمزنگاری مبدأ تا مقصد مجاز می‌باشد.

[۵] End to End Encryption

۵-۱-۱۰- تراکنش‌های فاقد رمزنگاری از مبدأ تا مقصد در ابزارهای پذیرش بدون حضور کارت، صرفاً باید با اتکا به زیرساخت فراهم آمده در سامانه پیوند و از طریق شماره تلفن همراه به جای شماره کارت انجام شود و شماره کارت در بسترهای فاقد رمزنگاری مبدا تا مقصد نباید انتقال یابد.

۵-۱-۱۱- در ابزار پذیرش بدون حضور کارت و فاقد رمزنگاری مبدأ تا مقصد، تنها ارائه سرویس‌های شارژ، قبض خدماتی و خیریه مجاز می‌باشد.

۵-۱-۱۲- به هنگام استفاده از ابزارهای پذیرش در تراکنش‌های با حضور کارت و بدون حضور کارت، باید صرفاً نام شرکت ارائه‌دهنده خدمات پرداخت و شرکت پرداخت‌یار به کاربران نمایش داده شود.

۵-۱-۱۳- شرکت‌های ارائه‌دهنده خدمات پرداخت موظف هستند برنامک همراه خود را به نام خود شرکت ارائه‌دهنده خدمات پرداخت و صرفاً از طریق درگاه‌های معتبر و اصیل ارائه دهند.

۵-۱-۱۴- شرکت ارائه‌دهنده خدمات پرداخت موظف است، در صورت درخواست ممیزان شاپرک، تمامی شواهد و مستندات مرتبط با الزامات سند حاضر را در اختیار آن‌ها قرار دهد.

۵-۲- الزامات عمومی ابزارهای پذیرش

۵-۲-۱- ابزار پذیرش با حضور کارت – الزامات عمومی

۵-۲-۱-۱- تنها ابزارهای پذیرش با حضور کارت دارای گواهینامه PCI-PTS معتبر[۶]، گواهی EMV Contact L1 & L2 و EMV Contactless L1 معتبر[۷] و نیز دارای تأییدیه شرکت شاپرک، در شبکه شاپرک قابل به‌کارگیری است. گواهینامه‌های فوق نیز تا تاریخ انقضای آن‌ها مورد تأیید شرکت شاپرک می‌باشد و چنانچه انجمن‌های PCI و EMV اقدام به تمدید آن‌ها نمایند، شرکت ارائه‌دهنده خدمات پرداخت مجاز به استفاده از ابزارهای مربوطه بوده و در صورت عدم تمدید، به‌کارگیری آن ابزارها در شبکه شاپرک غیرمجاز است.

۵-۲-۱-۲- برنامه کاربردی پرداخت ارائه شده توسط شرکت ارائه دهنده خدمات پرداخت باید قابلیت تشخیص رفتارهای غیرعادی و تلاش کاربران غیرمجاز به‌منظور دسترسی به اطلاعات و منابع حساس را داشته باشد. شرکت ارائه دهنده خدمات پرداخت باید تمهیدات لازم جهت ارائه پاسخ مناسب به این‌گونه رفتارها را در برنامه کاربردی پرداخت اعمال نماید. پاسخ مناسب به رفتارهای مذکور مانند و نه محدود به "محدودسازی دسترسی به منوهای پذیرنده و پشتیبان درصورت ورود رمز اشتباه بیش از حد مجاز"، "جلوگیری از تلاش غیرمجاز برای تغییر کلید"، "اطمینان از اینکه تغییرات مربوط به ابزارهای POI متصل به ابزار پذیرش فقط از طریق منوی پشتیبان (سوپروایزر) قابل انجام باشد" می‌باشد.

---

[۶] در سایت رسمی PCI-SSC لیست به‌روز دستگاه‌های دارای گواهی معتبر PCI-PTS قابل مشاهده است.

[۷] در سایت EMVCO لیست به روز دستگاه‌های دارای گواهی معتبر EMV L1 & L2 قابل مشاهده است.

۵-۲-۱-۳- شرکت ارائه دهنده خدمات پرداخت موظف است از قراردادن هرگونه رمز عبور به صورت هاردکد[۸] در پایانه‌های فروش اجتناب نماید.

توصیه: توصیه می‌گردد شرکت ارائه دهنده خدمات پرداخت در صورت وجود رمز پیش‌فرض پذیرنده، تمهیدات نرم‌افزاری را به کار گیرد تا پذیرنده ملزم به تغییر آن رمز در اولین استفاده باشد.

۵-۲-۱-۴- شرکت ارائه دهنده خدمات پرداخت باید دارای سامانه مدیریت ترمینال[۹] به منظور کنترل از راه دور پایانه‌ها باشد. اقداماتی از قبیل نصب، به‌روزرسانی یا حذف برنامه‌های کاربردی، اعمال پاسخ مناسب و سریع به تهدیدات امنیتی یا هرگونه رفتار مشکوک، توقف فعالیت پایانه در صورت صلاحدید و اعمال تنظیمات/تغییرات ارتباطی پایانه می‌بایست صرفاً از طریق سامانه مدیریت ترمینال صورت پذیرد. در صورت عدم وجود سامانه مدیریت ترمینال برای برخی از ابزارهای پذیرش، اعمال تمامی اقدامات بند حاضر توسط سایر سامانه‌های مرتبط در شرکت ارائه‌دهنده خدمات پرداخت الزامی‌است.

۵-۲-۱-۵- سامانه مدیریت ترمینال (TMS) اختصاص یافته به شرکت ارائه دهنده خدمات پرداخت باید دارای گواهی تست نفوذ از شرکت کاشف یا شرکت‌های مورد تأیید افتا باشد.

۵-۲-۱-۶- شرکت ارائه دهنده خدمات پرداخت موظف است دسترسی پشتیبانان پایانه فروش را با استفاده از رمز یکبار مصرف[۱۰] میسر نموده و لاگ‌ها[۱۱] و سوابق تمامی فعالیت‌های پشتیبانان، تاریخ و زمان انجام فعالیت‌های ایشان را ذخیره نماید. لاگ‌های مذکور می‌بایست به SOC شرکت ارائه‌دهنده خدمات پرداخت نیز ارسال گردند. لازم به ذکر است، پشتیبانان می‌بایست به تفکیک کد ملی یا دیگر شاخص‌های یکتا مشخص گردند و ارسال رمز یکبار مصرف برای نقش پشتیبان - بدون توجه به موجودیت یکتای شخص پشتیبان - مورد پذیرش نمی‌باشد.

۵-۲-۱-۷- در صورتی‌که شرکت ارائه دهنده خدمات پرداخت در کنار پایانه فروش از دستگاه‌های POI [۱۲] بهره برداری نماید، ملزم به ارائه گواهینامه PCI PTS معتبر و به ازای هر دستگاه POI و نیز اخذ تأییدیه شاپرک می‌باشد. (استفاده از دستگاه‌های POI متفرقه مجاز نمی‌باشد.)

۵-۲-۱-۸- شرکت ارائه دهنده خدمات پرداخت ضمن دارا بودن مسئولیت حراست از دستگاه‌های POI، موظف است بر اساس فهرستی از POIهای مجاز، دستگاه POI را از هرگونه تعویض، تغییر یا دستکاری غیرمجاز محافظت نموده و نسبت به عملکرد صحیح آن اطمینان حاصل نماید.

تذکر: لیست POIهای مجاز هر شرکت باید شامل نام سازنده، مدل دستگاه، شماره تأییدیه PTS، تأییدیه شاپرک، نسخه نرم‌افزاری و شماره سریال دستگاه باشد.

۵-۲-۱-۹- برنامه کاربردی پرداخت ارائه شده توسط شرکت ارائه دهنده خدمات پرداخت باید حداقل لاگ‌های ذیل را به صورت کامل و دقیق ثبت نماید.

---

[۸] Hardcode

[۹] TMS: Terminal Management System

[۱۰] OTP: One-time password

[۱۱] logs

[۱۲] Point of interaction

- فعال/غیرفعال نمودن هرگونه قابلیت/عملکرد خاص در پایانه فروشگاهی
- ثبت تلاش‌های اصالت‌سنجی ناموفق و غیرمجاز
- غیرفعال نمودن، حذف یا تغییر یک کنترل امنیتی

تذکر: لاگ‌های ثبت شده می‌بایست غیرقابل تغییر باشند و تنها کاربرانِ مجاز به آن‌ها دسترسی داشته باشند. همچنین، لاگ‌های مذکور می‌بایست به SOC شرکت ارائه‌دهنده خدمات پرداخت نیز ارسال گردند. بدیهی است اقلام اطلاعاتی حساس کارت نباید در لاگ‌ها مشاهده گردد.

۵-۲-۱-۱۰- شرکت ارائه‌دهنده خدمات پرداخت باید به تفکیک مالک ابزارهای پذیرش (اعم از شرکت ارائه‌دهنده خدمات پرداخت یا شرکت‌های طرف قرارداد (در حوزه فروش) یا مالکیت غیر)، شناسنامه آماری تمامی ابزارهای پذیرش با حضور کارت متصل و غیرمتصل خود را تهیه نماید. حداقل مشخصات لازم به منظور تهیه این شناسنامه به قرار زیر می‌باشد:

- تعداد کل
- نوع اتصال (Dial up، LAN، GPRS، Bluetooth و فروشگاهی)
- نسخه نرم‌افزار
- Hardware No
- Firmware No
- PCI-PTS Version
- تاریخ اعتبار گواهینامه
- Approval No
- وضعیت پشتیبانی از EMV
- وضعیت فعال بودن نرم‌افزار مربوط به امکانات EMV
- برند
- مدل/ سری دستگاه
- کشور سازنده
- نام شرکت سازنده خارجی
- نام شرکت تامین‌کننده داخلی
- بازاریابی داخلی
- شماره و تاریخ نامه تأییدیه شاپرک
- بانک‌های طرف قرارداد (هر کدام به تفکیک تعداد استفاده شده)

تذکر: مشخصه «بانک‌های طرف قرارداد»، فقط برای ابزارهای پذیرش با حضور کارت متصل، کاربردپذیر است.

۵-۲-۱-۱۱- این شناسنامه باید در صورت حداقل تغییر در هر یک از موارد فوق، به‌روزرسانی شده و پس از به تأیید رسیدن توسط مقام ارشد سازمان، ممهور به مهر شرکت گردد. شرکت‌های ارائه‌دهنده خدمات پرداخت پیش از اقدام به خرید ابزارهای پذیرش،

باید مجوز بهره‌برداری ابزار پذیرش را اعم از جدید یا ابزارهای پذیرش که نمونه‌های مشابه آن‌ها قبلاً تأیید شده است، از شرکت شاپرک اخذ نمایند.

تذکر: پس از تأیید نمونه اولیه، در صورتی که با بررسی و تست نمونه‌ای از این دستگاه در شبکه پرداخت کشور، هرگونه عدم انطباقی با الزامات مربوطه شرکت شاپرک مشاهده گردد و یا شرایط انطباق با الزامات ابزار پذیرش و گواهی PCI-PTS بر روی دستگاه احراز نشود، تأییدیه ارائه شده توسط شرکت شاپرک، متناسب با مورد عدم انطباق، به صورت جداگانه (برای یک نمونه ابزار پذیرش) و یا جمعی (برای تمامی ابزارهای پذیرش مشابه نمونه اولیه) ملغی خواهد گردید.

۵-۲-۱-۱۲- شرکت ارائه دهنده خدمات پرداخت باید با در نظر گرفتن مستند «الزامات امنیت اطلاعات شاپرک»، نسبت به حذف کامل اطلاعات حساس کارت از حافظه موقت، RAM, logfile و غیره و همچنین غیر قابل بازیابی بودن این اطلاعات، اطمینان حاصل نماید.

۵-۲-۲- ابزار پذیرش با حضور کارت-فرایند تأیید ابزار پذیرش

۵-۲-۲-۱- شرکت ارائه‌دهنده خدمات پرداخت باید طی مکاتبهٔ رسمی با شرکت شاپرک، ابزار پذیرشی که قصد خرید آن را دارد معرفی نموده و دو نمونه از دستگاه ابزار پذیرش جدید را به همراه مدارک و ملزومات زیر به شرکت شاپرک ارسال نماید:

۱- نامه «معرفی نمونه دستگاه کارتخوان»، خطاب به "مدیریت صدور مجوز و اعمال مقررات" شرکت شاپرک، با موضوع «درخواست تأیید دستگاه کارتخوان» همراه با درج سریال دستگاه، نشان تجاری و مدل دستگاه مورد درخواست

۲- کاتالوگ منطبق با نمونه دستگاه ارسالی به شاپرک

۳- اظهارنامه الکترونیکی دارای شماره سریال(شماره کوتاژ)[۱۳] با مالکیت شخص حقوقی تامین کننده (ضروری است اطلاعات زیر به صورت خوانا در سند قابل رویت باشد)

- ❖ نام شرکت تأمین‌کننده
- ❖ شرح کالا
- ❖ کد کالا
- ❖ تاریخ اظهار
- ❖ شماره قبض انبار
- ❖ شماره پیگیری انبار
- ❖ شماره بارنامه
- ❖ کد ثبت سفارش

۴- وجود و اصالت برچسب گارانتی بر روی بدنه دستگاه[۱۴]

۵- اصل گواهی PCI-PTS دستگاه

۶- اصل گواهی EMV سطح ۱ و ۲

---

[۱۳] Cottage

[۱۴] مطابق با الزامات سخت افزار بدنه بند (۳-۲-۱-۷)

۷- مستند نحوه به‌کارگیری دستگاه[۱۵]

۸- تأییدیه سازمان تنظیم مقررات رادیویی کشور

۹- مدارک و مستندات زیر در صورت وجود به همراه تأییدیه سازمان تنظیم مقررات رادیویی کشور، به پیوست نامه نیز ارسال گردد:

- ❖ نتایج نهایی آزمون EMC
- ❖ نتایج نهایی آزمون SAR
- ❖ نتایج نهایی آزمون Safety
- ❖ نتایج نهایی آزمون RF
- ❖ تأییدیه سازمان تنظیم مقررات رادیویی کشور با «موضوع تأیید نمونه آزمون»

۱۰- هرگونه رمز عبور لازم جهت ورود به منوهای کاربری، پیکربندی و مدیریت ابزار پذیرش

۱۱- مستند نحوه رؤیت اطلاعات فنی از جمله نسخه سیستم عامل، Firmware، EMV Kernel و PCI-PTS روی ابزار پذیرش

۱۲- اطلاعات تماس فرد پاسخگو به شاپرک در خصوص ابزار پذیرش

۱۳- راهنمای کاربری سخت‌افزاری و نرم‌افزاری مورد استفاده پذیرنده به زبان فارسی

۱۴- تدوین دفترچه نکات امنیتی و حفاظتی ابزار پذیرش برای ارائه به پذیرندگان به زبان فارسی

۱۵- مستند رویه مدیریت کلید ابزار پذیرش

۱۶- سند مشخصات سخت‌افزاری و نرم‌افزاری[۱۶]

۱۷- در صورتی که ابزار ارسالی M-POS، PIN-PAD یا OEM EPP [۱۷] باشد، راهکار نهایی شامل سخت‌افزار و نرم‌افزار مورد استفاده در ابزار پذیرش توسط شرکت ارائه‌دهنده خدمات پرداخت، باید به صورت جداگانه تأییدیه شرکت شاپرک را دریافت نماید.

۱۸- نمونه دستگاه‌های جدید باید شامل تمامی اقلام جانبی مربوطه از قبیل پایه، کابل‌های ارتباطی، تجهیزات تأمین توان (باتری، شارژر، آداپتور)، صفحه کلید، نمایشگر جانبی و سایر متعلقات و ملزومات باشد. ضمناً نمونه‌های ارسالی که سابقه تأیید قبلی دارند باید شامل برنامه کاربردی پرداخت[۱۸] شرکت ارائه‌دهنده خدمات پرداخت بوده و آماده به‌کارگیری در شبکه پرداخت باشند.

۵-۲-۲-۲- مراحل تحویل نمونه دستگاه به شرکت شاپرک و تأیید آن توسط شاپرک به شرح گام‌های ذیل می‌باشد:

۱- نماینده شرکت ارائه دهنده خدمات پرداخت (متقاضی) به منظور تحویل نمونه دستگاه و اسناد مندرج در بند (۵-۲-۲-۱)، هماهنگی لازم را با مدیریت صدور مجوز و مقررات شرکت شاپرک به عمل می‌آورد.

---

[۱۵] Manual

[۱۶] Data Sheet

[۱۷] Original Equipment Manufacturer Encryption Pin Pad

[۱۸] Payment Application

۲- نماینده شرکت شاپرک طی هماهنگی با نماینده متقاضی، نسبت به تنظیم زمان جلسه با عنوان «تحویل دستگاه کارتخوان» اقدام می‌نماید.

۳- در جلسهٔ «تحویل دستگاه کارتخوان» بررسی اولیه کفایت اسناد و مدارک مندرج در بند (۵-۲-۲-۱) انجام می‌شود و در صورت کفایت مدارک، دستگاه به همراه مدارک مربوطه از نماینده متقاضی تحویل گرفته می‌شود. در صورت وجود نقص در مدارک، نمونه دستگاه کارتخوان به همراه کلیه اسناد و مدارک به نماینده شرکت متقاضی عودت داده می‌شود.

۴- تأییدیهٔ کفایت مدارک و دریافت نمونه دستگاه، علاوه بر تنظیم و امضای صورتجلسهٔ تحویل، از طریق مکاتبه رسمی به شرکت متقاضی اطلاع رسانی خواهد شد.

۵- پس از بررسی و صحت‌سنجی مدارک دریافتی، از نماینده شرکت متقاضی به همراه کارشناس مطلع و دارای دسترسی لازم جهت کنترل اظهارنامه گمرکی و سایر اسناد مربوطه دعوت به عمل می‌آید.

۶- در هر زمان و هر مرحله تعریف شده، در صورت عدم احراز صحت مدارک ارائه شده یا عدم احراز شرایط امنیتی و فنی مورد نظر شرکت شاپرک، مدیریت صدور مجوز و اعمال مقررات نسبت به صدور نامه عدم تأیید درخواست مشتمل بر موارد عدم پذیرش اقدام می‌نماید.

۷- در صورت احراز تمامی شرایط مورد نظر شرکت شاپرک، نامه تأیید بهره‌برداری دستگاه نمونه ارسالی، توسط مدیریت صدور مجوز و اعمال مقررات صادر می‌گردد.

۸- شرکت شاپرک ظرف مدت ۱۴ روز تقویمی از تاریخ برگزاری جلسهٔ «تحویل دستگاه کارتخوان»، نسبت به اعلام نتیجه قطعی مبنی بر تأیید یا عدم تأیید اجازه بهره‌برداری از دستگاه کارتخوان موردنظر در شبکه پرداخت کشور به شرکت ارائه دهنده خدمات پرداخت اقدام می‌نماید. همچنین نتیجه بررسی از طریق مکاتبه رسمی به متقاضی اطلاع‌رسانی خواهد شد.

۵-۲-۲-۳- تمام تجهیزات جانبی و متعلقات ابزار پذیرش باید با مستندات فنی دستگاه مطابقت داشته و به تأیید آزمایشگاه سخت‌افزار شرکت شاپرک رسیده باشد.

۵-۲-۲-۴- درخصوص سخت‌افزار بدنه ابزار پذیرش رعایت موارد زیر الزامی است:

- همه پیچ‌های بدنه باید در جای خود بسته و محکم شده باشد (استفاده از ابزار مجهز به تُرک‌متر[۱۹] الزامی است).
- حداقل یکی از پیچ‌های اتصال قاب بدنه یا محل مناسبی در بدنه ابزار پذیرش باید با برچسب گارانتی محافظت شود؛ به نحوی که دسترسی به سخت‌افزار داخلی باعث مخدوش شدن برچسب گردد. در مورد ابزار پذیرش تعمیر شده، برچسب باید منقوش به لوگوی شرکت بوده و نمونه آن به تأیید شاپرک رسیده باشد.
- ترمیم شکستگی‌های قطعات بدنه تحت هیچ شرایطی جایز نیست.
- جنس بدنه ابزار پذیرش باید مانع رؤیت سخت‌افزار داخلی باشد. پوشش و حذف شفافیت بدنه به‌واسطه رنگ‌آمیزی یا سایر روش‌های برگشت‌پذیر قابل قبول نیست.
- برداشتن قطعات تفکیک‌پذیر بدنه ابزار پذیرش نباید امکان دسترسی به مدارات و بردهای امنیتی را ایجاد کند.

[۱۹] Torque Meter

- وجود فاصله هوایی بین قطعات بدنه ابزار پذیرش به نحوی که امکان یا احتمال ورود به سخت‌افزار وجود داشته باشد، مجاز نیست.

۵-۲-۵- برچسب مشخصات اختصاصی ابزار پذیرش باید واضح بوده و از استحکام کافی برخوردار باشد. انواع شارژر دستگاه‌های سیار، منابع تغذیه (آداپتورها) و باتری ابزارهای پذیرش با حضور کارت، الزاماً باید متناسب با مشخصات دستگاه و دارای گواهی استاندارد ملی باشد.

۵-۲-۶- مستند فرآیند به‌روزرسانی ابزارهای پذیرش با حضور کارت باید به تفکیک برند و مدل تهیه شود. در این مستند، چگونگی به‌روزرسانی هریک از موارد زیر باید ذکر شده باشد.

- سیستم عامل
- نرم‌افزار (فرایندهای تغییر نسخه)
- اطلاعات پیکربندی (فرایند چگونگی تغییر مشخصات پذیرنده)

۵-۲-۷- مستند انطباق با دستگاه‌های تأیید شده در سایت انجمن PCI برای تمامی ابزارهای پذیرش با حضور کارت متصل و غیرمتصل شرکت ارائه‌دهنده خدمات پرداخت باید تهیه شود. مستند مذکور باید حداقل شامل موارد زیر باشد:

- نام شرکت سازنده
- شماره میان‌افزار
- شماره سخت‌افزار
- Approval Number
- Approval Class
- Version
- Expiry Date
- PIN Support
- Key Management
- PIN Entry Technology

این مستند باید تمامی انواع ابزارهای پذیرش با حضور کارت شرکت ارائه دهنده خدمات پرداخت را پوشش دهد.

۵-۲-۸- مستند انطباق با دستگاه‌های تأیید شده در سایت EMV برای تمامی ابزارهای پذیرش با حضور کارت متصل و غیرمتصل شرکت ارائه دهنده خدمات پرداخت باید تهیه شود. مستند مذکور باید حداقل شامل موارد زیر باشد:

- نام شرکت سازنده
- نسخه میان‌افزار
- نسخه سخت‌افزار
- Approval Number(s) (به ازای هر دو گواهی EMV L1 و EMV L2 برای دستگاه‌های تماسی و به ازای گواهی EMV دستگاه‌های غیرتماسی)
- EMV Application Kernel
- Operating System
- Expiry Date

این مستند باید تمامی انواع ابزارهای پذیرش با حضور کارت شرکت ارائه‌دهنده خدمات پرداخت را پوشش دهد.

۵-۲-۲-۹- شماره سریال مندرج بر روی برچسب مشخصات دستگاه و شماره سریال روی برچسب مشخصات جعبه (دستگاه‌های جدید)، باید منحصربه‌فرد و با شماره سریالی که از سخت‌افزار استخراج می‌شود منطبق باشد[۲۰]. مشخصات الکتریکی، ارتباطی و سایر مندرجات برچسب با اطلاعات مشابه در داخل دستگاه باید مطابقت داشته باشند.

۵-۲-۲-۱۰- ابزار پذیرش با حضور کارت باید دارای صفحه کلید فارسی یا انگلیسی باشد.

۵-۲-۲-۱۱- ابزار پذیرش با حضور کارت باید صرفاً حروف و اعداد زبان فارسی یا انگلیسی را در صفحه نمایش دستگاه نمایش داده و بر روی رسید چاپ نماید.

۵-۲-۲-۱۲- ابزارهای پذیرش با حضور کارت باید هر دو امکان استفاده با کارت مغناطیسی و هوشمند را داشته باشد.

۵-۲-۲-۱۳- برنامه‌های کاربردی نصب شده روی دستگاه‌های پایانه فروش هوشمند (PDA POS) می‌بایست محدود به برنامه‌های مورد نیاز برای انجام تراکنش پرداخت کارتی باشد. نصب هرگونه برنامه جانبی و غیرمرتبط با پرداخت کارتی بر روی این دستگاه‌ها ممنوع است. این نرم‌افزارها شامل و نه محدود به برنامه‌های نصب شده و سرویس‌های سیستم عامل می‌باشد.

۵-۲-۲-۱۴- دستگاه باید در هنگام روشن شدن، مراحل Self-Test را به‌صورت خودکار انجام داده و هرگونه تغییرات سخت‌افزاری یا نرم‌افزاری غیر استاندارد را تشخیص داده و در صورت وقوع، از ورود به شبکه ممانعت به عمل آورد. لازم به ذکر است طبق الزامات PCI-PTS، فرآیند Self-Test باید هر ۲۴ ساعت یکبار انجام شود.

۵-۲-۲-۱۵- رمز کارت مشتری بعد از ورود آن از طریق صفحه کلید ابزار پذیرش با حضور کارت، به هنگام ارسال یا کاربردهای دیگر، باید به صورت رمز شده و منطبق با الزامات PCI-PTS باشد.

۵-۲-۲-۱۶- نمایش رمز کارت مشتری بر روی صفحه نمایش، در زمان ورود از طریق صفحه کلید ابزار پذیرش با حضور کارت غیرمجاز است.

۵-۲-۲-۱۷- مبلغ تراکنش باید روی ابزار پذیرش و پیش از ورود رمز به رؤیت و تأیید دارنده کارت برسد.

۵-۲-۲-۱۸- درصورتی‌که ابزار پذیرش با حضور کارت دارای SAM Module باشد، کلیدهای رمزنگاری باید در این حافظه نگهداری شوند؛ در غیر این صورت نگهداری کلیدهای رمز در حافظه ابزار پذیرش با حضور کارت باید با استفاده از رمزنگاری انجام گرفته و لازم است بخش رمزنگاری قوی مطابق با سند «الزامات امنیت اطلاعات شاپرک» رعایت شود.

۵-۲-۲-۱۹- هر ابزار پذیرش با حضور کارت باید کلید رمز منحصربه‌فرد داشته باشد و استفاده از کلید رمز تکراری مجاز نمی‌باشد.

۵-۲-۲-۲۰- ابزار پذیرش با حضور کارت باید به درستی نصب، مدیریت و محافظت شود به گونه‌ای که تمامی ریسک‌های حملاتی همچون دزدی و دستکاری غیرقانونی ابزار پذیرش با حضور کارت را پوشش دهد. شرکت ارائه‌دهنده خدمات پرداخت موظف است پذیرنده را متعهد نماید در صورت مشاهده هرگونه مورد یا ابزار مشکوک نصب شده روی ابزار پذیرش با حضور کارت، در اسرع وقت شرکت ارائه‌دهنده خدمات پرداخت را مطلع نماید.

---

[۲۰] شرکت‌های ارائه دهنده خدمات پرداخت باید دقت نمایند درصورت اعمال کنترل‌های این سند بر روی سوئیچ شرکت شاپرک، چنانچه شماره سریال اعلامی از طرف شرکت ارائه‌دهنده خدمات پرداخت-مذکور در این بند- با شماره سریال ارسالی از طرف ابزار پذیرش بر روی سوئیچ شاپرک در هنگام اجرای تراکنش، تطابق نداشته باشد، سوئیچ شاپرک از اجرای تراکنش ممانعت به عمل خواهد آورد.

۵-۲-۲-۲۱- به منظور آموزش نحوه استفاده از دستگاه، شرکت ارائه‌دهنده خدمات پرداخت باید مستند آموزش نحوه کارکرد دستگاه را تهیه و به پذیرندگان ارائه نماید. این مستند باید تمامی منوها و زیر منوهای نرم‌افزار دستگاه، به همراه موارد امنیتی که لازم است پذیرنده آگاهی داشته باشد را توضیح دهد.

۵-۲-۲-۲۲- منوی ابزار پذیرش با حضور کارت باید در انطباق کامل با الزامات مندرج در سند «یکسان‌سازی منوی پایانه‌های فروش» باشد.

۵-۲-۲-۲۳- در تأمین امنیت نرم‌افزار ابزار پذیرش با حضور کارت، رعایت بخش امنیت نرم‌افزار تولید داخل سازمان از سند «الزامات امنیت اطلاعات شاپرک» الزامی است.

۵-۲-۲-۲۴- نحوه ارائه رسید توسط دستگاه پایانه فروش باید مطابق با مقررات «صدور برگه رسید پایانه‌های فروش» و «مقررات صدور رسیدهای الکترونیکی در پرداخت‌های الکترونیکی مبتنی بر کارت» باشد. شرکت ارائه‌دهنده خدمات پرداخت باید برای پایانه‌هایی که رسید دیجیتال صادر می‌نمایند، دمو از نحوه صدور رسید توسط دستگاه به شرکت شاپرک ارائه کند.

۵-۲-۲-۲۵- لازم است شرکت ارائه دهنده خدمات پرداخت مکانیزمی فراهم نماید تا پذیرندگان فروشگاهی دارای دستگاه‌های کارتخوان Dial-up تنها امکان استفاده از خط تلفن تعریف شده (خط تلفن پذیرنده) در سامانه‌های شرکت ارائه دهنده خدمات پرداخت را داشته باشند، به نحوی که در صورت مغایرت در استفاده از خط تلفن، امکان گزارش‌گیری و تحلیل آن در سامانه‌های تشخیص تقلب شرکت ارائه دهنده خدمات پرداخت فراهم باشد.

۵-۲-۲-۲۶- سیم‌کارت دستگاه کارت‌خوان سیار می‌بایست متعلق به پذیرنده و از نوع «Data» باشد به نحوی که رومینگ آن غیرفعال بوده و هیچ سیم‌کارت دیگری غیر از سیم‌کارت تعریف شده در سامانه‌های شرکت ارائه‌دهنده خدمات پرداخت، امکان تراکنش بر روی دستگاه را نداشته باشد.

۵-۲-۲-۲۷- شرکت ارائه دهنده خدمات پرداخت باید ترکیب منحصربفرد:

- شماره سریال دستگاه (اعم از Dial-up، GPRS، LAN و WLAN)
- شماره تلفن/شماره سیم‌کارت
- شماره ترمینال

را در خصوص هر پایانه فروش فعال در شبکه پرداخت کشور نگهداری و در صورت لزوم به روزرسانی نماید.

۵-۲-۲-۲۸- شرکت ارائه‌دهنده خدمات پرداخت می‌بایست مکانیزمی فراهم نماید تا دستگاه‌های کارت‌خوان متعلق به شرکت ارائه دهنده خدمات پرداخت در خارج از مرزهای جغرافیایی ایران امکان تراکنش نداشته باشند.

۵-۲-۳- الزامات نرم‌افزار پایانه فروش با سیستم عامل اندروید

شرکت ارائه دهنده خدمات پرداخت در پایانه‌های فروش با سیستم‌عامل اندروید، باید الزامات زیر را لحاظ نماید.

۵-۲-۳-۱- حالت سیستمی TEE[۲۱] سخت‌افزاری (مثل Knox برای دستگاه‌های سامسونگ) یا EMM[۲۲] می‌بایست در سیستم عامل پایانه فروش فعال باشد.

۵-۲-۳-۲- سیستم عامل پایانه فروش می‌بایست صرفاً شامل نرم‌افزارهای (برنامه‌ها و سرویس‌ها) ضروری برای عملیات پرداخت از طریق پایانه فروش باشد. همچنین سیستم عامل پایانه فروش می‌بایست به صورت امن پیکربندی شده باشد و با حداقل مجوز دسترسی اجرا شود.

۵-۲-۳-۳- امکان به روزرسانی و هاردنینگ سیستم عامل پایانه فروش برای پذیرنده نباید وجود داشته باشد، همچنین هر نوع دسترسی و دستکاری سیستم عامل، برنامه کاربردی یا Firmware توسط پذیرنده غیرمجاز است.

۵-۲-۳-۴- حذف برنامه‌های نصب شده بر روی پایانه فروش و اطلاعات وابسته به آن‌ها نباید بدون مجوز از شرکت ارائه‌دهنده خدمات پرداخت، امکان‌پذیر باشد.

۵-۲-۳-۵- نصب[۲۳] یا بارگذاری[۲۴] هرگونه برنامه کاربردی روی پایانه فروش، صرفاً می‌بایست توسط ابزار رمزنگاری ارائه شده توسط تولیدکننده پایانه فروش[۲۵]، امضا شود و شرکت ارائه دهنده خدمات پرداخت تنها مجاز به میزبانی از برنامه‌های کاربردی امضا شده خود در پایانه‌های فروش اندرویدی می‌باشد. نام و مشخصات این ابزار باید در اختیار شرکت شاپرک قرار داده شود، همچنین این ابزار نباید در اختیار غیر قرار گیرد و مسئولیت هرگونه سوء استفاده از آن به عهده شرکت ارائه‌دهنده خدمات پرداخت می‌باشد.

۵-۲-۳-۶- شرکت ارائه دهنده خدمات پرداخت می‌بایست مستند نحوه به‌روزرسانی سیستم عامل Firmware و برنامه کاربردی پایانه فروش را تهیه نموده و در اختیار شرکت شاپرک قرار دهد.

۵-۲-۳-۷- شرکت ارائه دهنده خدمات پرداخت می‌بایست مستند مدیریت کلید بر روی پایانه فروش را تهیه نموده و در اختیار شرکت شاپرک قرار دهد.

۵-۲-۳-۸- شرکت ارائه دهنده خدمات پرداخت می‌بایست تمهیدات قراردادی و پشتیبانی را به گونه‌ای اتخاذ نماید تا در صورت وجود آسیب‌پذیری بر روی Firmware ، امکان دریافت به‌روزرسانی آن از تولیدکننده پایانه فروش وجود داشته باشد.

۵-۲-۳-۹- لاگ فعالیت‌های مدیریتی و امنیتی (از جمله مدیریت کلید) بر روی پایانه فروش، می‌بایست سمت سرور مربوطه در شرکت ارائه دهنده خدمات پرداخت، ثبت و نگهداری شود. رعایت الزامات مربوط به مدت زمان و محل نگهداری و ارسال لاگ به سامانه SOC شرکت ارائه دهنده خدمات پرداخت مطابق با سند «الزامات امنیت اطلاعات شاپرک» الزامی است.

۵-۲-۳-۱۰- لاگ فعالیت‌های سوپروایزر (پشتیبان) بر روی پایانه فروش می‌بایست در سامانه مربوطه در شرکت ارائه دهنده خدمات پرداخت ثبت و نگهداری شود. رعایت الزامات مربوط به مدت زمان و محل نگهداری و ارسال لاگ به سامانه SOC شرکت ارائه دهنده خدمات پرداخت مطابق با سند «الزامات امنیت اطلاعات شاپرک» الزامی است.

---

[۲۱] Trusted Execution Environment

[۲۲] Enterprise Mobility Management

[۲۳] Load

[۲۴] Installation

[۲۵] Vendor

۵-۲-۳-۱۱- در صورتی که امکان نصب چندین برنامه کاربردی پرداخت بر روی پایانه فروش وجود داشته باشد، تنظیمات پایانه فروش باید به گونه‌ای باشد که امکان دسترسی و یا دستکاری داده‌ها از طریق سایر برنامه‌های کاربردی پرداخت وجود نداشته باشد. لازم به ذکر است در این بند، برنامه کاربردی پرداخت به برنامه‌هایی اطلاق می‌شود که از طریق پایانه فروش امکان انجام پرداخت حضوری در آن فراهم شده است؛ از جمله برنامه پرداخت غیرتماسی، کیف پول، QR Code و غیره. انتقال وجه کارت به کارت و سایر روش‌های پرداخت بدون حضور کارت یا بدون حضور مشتری، برای مثال از طریق IPG، از طریق پایانه فروش مجاز نیست.

۵-۲-۳-۱۲- شرکت ارائه دهنده خدمات پرداخت می‌بایست مستند استفاده از پروتکل‌ها و سرویس‌های قابل استفاده در واسط‌های مختلف پایانه فروش (از جمله تجهیزات جانبی مانند و نه محدود به پرینتر و بلوتوث و غیره) توسط برنامه‌های کاربردی را تهیه نموده و در اختیار شرکت شاپرک قرار دهد.

۵-۲-۳-۱۳- شرکت ارائه دهنده خدمات پرداخت می‌بایست در صورت وجود چند برنامه کاربردی پرداخت مختلف بر روی پایانه فروش که ملزم به همکاری و انتقال پیام به یکدیگر هستند، پروتکل‌ها، دسترسی‌ها و نحوه عملکرد آنها را مستند نموده و در اختیار شرکت شاپرک قرار دهد.

۵-۲-۳-۱۴- شرکت ارائه دهنده خدمات پرداخت می‌بایست مستند راهنمای امن توسعه برنامه کاربردی پایانه فروش را تهیه نموده و در اختیار شرکت شاپرک قرار دهد.

۵-۲-۳-۱۵- برنامه کاربردی پرداخت نصب شده بر روی ابزار پذیرش باید وضعیت روت بودن (Root) دستگاه را بررسی نموده و در صورت روت بودن دستگاه، قابلیت اجرایی نداشته باشد.

۵-۲-۳-۱۶- شرکت ارائه دهنده خدمات پرداخت می‌بایست مستند نحوه عملکرد و رفتار سیستم پایانه فروش در هنگام نقض امنیت و در حین استفاده از برنامه کاربردی پرداخت را تدوین نموده و در اختیار شرکت شاپرک قرار دهد. به عنوان مثال در صورت تلاش برای دسترسی غیرمجاز به داده‌های حساس توسط مهاجم، پایانه فروش اطلاعات حیاتی را حذف نموده، سطح دسترسی را محدود نماید یا هشداری براساس نوع عمل مخرب به سرور مربوطه در شرکت ارائه دهنده خدمات پرداخت ارسال نماید.

۵-۲-۳-۱۷- شرکت ارائه دهنده خدمات پرداخت می‌بایست برنامه کاربردی پایانه فروش را مطابق با استانداردهای معتبر مانند و نه محدود به OWASP و NIST و با استفاده از توابع و کتابخانه‌های امن پروتکل‌ها و الگوریتم‌های پشتیبانی شده توسط پایانه فروش توسعه دهد. به علاوه تست نفوذ برنامه کاربردی می‌بایست مطابق با متدولوژی‌های استاندارد انجام شود.

۵-۲-۳-۱۸- شرکت ارائه‌دهنده خدمات پرداخت تنها مجاز به به‌کارگیری پایانه‌های فروش اندرویدی با نسخه‌های پایدار و به‌روز سیستم عامل اندروید می‌باشد. نسخه‌های پایدار و به‌روز سیستم‌عامل هر ساله توسط شرکت شاپرک اعلام می‌گردند.

۵-۲-۳-۱۹- شرکت ارائه دهنده خدمات پرداخت باید در طراحی و توسعه برنامه کاربردی پرداخت خود، انطباق با الزامات امنیتی مبتنی بر چارچوب PCI-SSF [۲۶] را لحاظ و مستند نماید. در صورتی که طراحی و توسعه برنامه کاربردی پرداخت توسط شرکت

[۲۶] PCI Software Security Framework

ثالث[۲۷] ارائه دهنده راهکارهای نرم‌افزاری انجام پذیرفته، شرکت ارائه دهنده خدمات پرداخت می‌بایست مستندات انطباق با الزامات چارچوب PCI-SSF را از شرکت ثالث همکار دریافت نماید.

۵-۲-۳-۲۰- شرکت ارائه دهنده خدمات پرداخت باید گواهی تأییدیه برنامه کاربردی پرداخت خود را از شرکت کاشف یا شرکت‌های مورد تأیید افتا به منظور پایبندی به الزامات حاضر اخذ نماید.

۵-۲-۳-۲۱- شرکت ارائه دهنده خدمات پرداخت موظف است، در صورت توسعه برنامه کاربردی پرداخت توسط شرکت ثالث همکار، ضمن نظارت مستمر بر توسعه برنامه کاربردی پرداخت، نسبت به code review برنامه کاربردی پرداخت ارائه شده اقدام نماید. همچنین باید منبع[۲۸] برنامه کاربردی پرداخت را در اختیار داشته و Build نسخه نیز در شرکت ارائه‌دهنده خدمات پرداخت انجام پذیرد.

۵-۲-۳-۲۲- شرکت ارائه دهنده خدمات پرداخت می‌بایست از فعال بودن سازوکار راه‌اندازی امن[۲۹] در پایانه‌های فروش اندرویدی به‌جهت جلوگیری از بوت شدن نرم‌افزارهای تأیید نشده و عدم دستکاری[۳۰] bootloader اطمینان حاصل کند.

۵-۲-۳-۲۳- شرکت ارائه دهنده خدمات پرداخت می‌بایست از تفکیک حافظه برنامه کاربردی پرداخت با سایر برنامه‌های کاربردی جانبی ارائه شده در پایانه فروش اندرویدی اطمینان حاصل نماید.

۵-۲-۳-۲۴- شرکت ارائه دهنده خدمات پرداخت باید از ارتباط امن برنامه‌های کاربردی جانبی با برنامه کاربردی پرداخت اطمینان حاصل نماید.

۵-۲-۳-۲۵- شرکت ارائه دهنده خدمات پرداخت باید از در اختیار بودن امکانات و دسترسی‌های ذیل صرفاً در برنامه کاربردی پرداخت اطمینان حاصل نماید.

- انجام تراکنش مالی
- دسترسی به حافظه امن
- دسترسی به چاپگر
- دسترسی برای خواندن انواع ابزارهای پرداخت از جمله انواع ابزارهای تماسی و غیر تماسی

۵-۲-۳-۲۶- شرکت ارائه دهنده خدمات پرداخت موظف است به منظور اطمینان از عملکرد صحیح برنامه کاربردی پرداخت، به ازای هربار تغییر نسخه عمده[۳۱]، فرایند آزمون‌های امنیتی و عملکردی را انجام داده و و سناریوها و نتایج آزمون را نگهداری نماید.

۵-۲-۳-۲۷- شرکت ارائه دهنده خدمات پرداخت موظف است تمامی تغییرات نسخه‌های برنامه کاربردی پرداخت را مستند و سوابق آن را نگهداری نماید.

---

[۲۷] Third party

[۲۸] Source

[۲۹] Android Secure Boot یک ویژگی امنیتی است که در دستگاه‌های اندرویدی گنجانده شده است و یکپارچگی برنامه‌کاربردی دستگاه را در هنگام راه‌اندازی تأیید می‌کند. این ویژگی، تضمین می‌کند که فقط نرم‌افزار معتبر و دارای امضا می‌تواند بارگیری شود، بنابراین به جلوگیری از بارگیری نرم‌افزارهای مخرب در سطح بوت و هسته کمک می‌کند.

[۳۰] untampered

[۳۱] Major changes

۵-۲-۳-۲۸- شرکت ارائه دهنده خدمات پرداخت باید پس از اضافه نمودن هر برنامه کاربردی جانبی جدید به پایانه فروش اندرویدی، ضمن انجام آزمون‌های امنیتی، مستندات و نتایج آزمون را نگهداری نماید.

۵-۲-۳-۲۹- شرکت ارائه دهنده خدمات پرداخت موظف است به منظور اطمینان از حفظ یکپارچگی نرم‌افزار، تمامی نسخه‌های پیشین برنامه کاربردی ارائه شده اعم از اینکه برنامه کاربردی توسط خود شرکت یا توسط شرکت‌های ثالث تدوین شده باشد را نگهداری نماید.

۵-۲-۳-۳۰- شرکت ارائه‌دهنده خدمات پرداخت تنها مجاز به بکارگیری پایانه های فروش اندرویدی است که تامین کننده آن، آپدیت‌ها و وصله های امنیتی را به صورت مستمر (حداقل ماهانه) ارائه نماید.

۵-۲-۳-۳۱- شرکت ارائه‌دهنده خدمات پرداخت باید مطابق مستند «الزامات امنیت اطلاعات شاپرک» حداقل ماهانه، اقدام به به‌روزرسانی و اعمال وصله‌های امنیتی نماید.

۵-۲-۳-۳۲- شرکت ارائه دهنده خدمات پرداخت باید با در نظر گرفتن مستند «الزامات امنیت اطلاعات شاپرک»، نسبت به حذف سرویس‌های غیرکاربردی و نیز غیرفعال نمودن پورت‌ها و بسترهای ارتباطی غیرضروری پایانه‌های اندرویدی مانند و نه محدود به بلوتوث اقدام نماید.

۵-۲-۳-۳۳- شرکت ارائه دهنده خدمات پرداخت موظف است قابلیت‌های ارائه شده توسط برنامه کاربردی پرداخت پایانه فروش اندرویدی را تنها زمانی به صورت پیش‌فرض فعال نماید که به‌صورت مستند و قابل توجیه، به‌عنوان بخشی از معماری برنامه کاربردی پرداخت تعریف نموده باشد و مغایر با الزامات شاپرک نباشند.

۵-۲-۴- درگاه پرداخت اینترنتی

۵-۲-۴-۱- شرکت ارائه دهنده خدمات پرداخت باید مستند تراکنش‌های اینترنتی را که حداقل شامل موارد زیر باشد، تدوین نماید.

- چگونگی انجام یک تراکنش اینترنتی
- دیاگرام سطح بالای جریان تبادل اطلاعات بین موجودیت‌های درگیر (سیگنالینگ تراکنش)
- نحوه هدایت مشتری تا انجام کامل تراکنش
- مکانیزم مطلع‌سازی پذیرنده از انجام موفق تراکنش
- چگونگی صدور رسید
- ارائه انواع پیغام‌های خطا در صفحه پرداخت اینترنتی
- نحوه مدیریت پیغام‌های خطا

۵-۲-۴-۲- تمامی تراکنش‌های اینترنتی الزاماً باید با استفاده از توکن انجام شود و تمامی روش‌های سنتی بدون دریافت توکن غیرمعتبر است. این توکن باید حداکثر به میزان ۱۵ دقیقه معتبر بوده و به صورت یکتا و تصادفی در هنگام انجام تراکنش با درخواست پذیرنده از طرف شرکت ارائه‌دهنده پرداخت به پذیرنده ارائه شود.

۵-۲-۴-۳- شرکت ارائه‌دهنده خدمات پرداخت کارت موظف است منحصراً برای آدرس IPهای مشخص و محدود شدهٔ متعلق به پذیرنده اینترنتی مجاز طبق سند «الزامات پذیرندگان اینترنتی» درگاه پرداخت اینترنتی اختصاص دهد. ارائه درگاه پرداخت اینترنتی توسط شرکت ارائه‌دهنده خدمات پرداخت برای آدرس IP نامحدود و نامشخص ممنوع است.

۵-۲-۴-۴- شرکت ارائه‌دهنده خدمات پرداخت باید صرفاً به درخواست‌های ارسالی از طریق URLهایی پاسخ دهد که دقیقاً در سامانه جامع پذیرندگان شاپرک به عنوان آدرس اینترنتی آن پذیرنده ثبت شده باشد. همچنین لازم است شرکت ارائه‌دهنده خدمات پرداخت هرگونه تغییرات درخواستی از طرف پذیرنده در آدرس URL را، پس از اعمال کنترل‌های لازم انجام دهد.

۵-۲-۴-۵- شرکت ارائه‌دهنده خدمات پرداخت باید نام دامنه فراخواننده درگاه[۳۲] را با آدرس URL ثبت شده پذیرنده مطابقت داده و درصورت یکسان بودن آن‌ها اجازه انجام تراکنش را صادر نماید.

۵-۲-۴-۶- شرکت ارائه‌دهنده خدمات پرداخت باید صرفاً به درخواست‌هایی که آدرس Callback URL آنها با آدرس ثبت شده پذیرنده یکسان بوده یا زیردامنه آن باشد اجازه انجام تراکنش بدهد.

تذکر: برای شرایطی که این موضوع قابل اجرا نیست، لازم است موارد به شرکت شاپرک اطلاع‌رسانی و تایید اخذ شود.

۵-۲-۴-۷- به منظور تأمین امنیت ارتباط درگاه پرداخت اینترنتی، رعایت الزامات امنیت ارتباط با سرویس‌های اینترنتی مطابق با سند «الزامات امنیت اطلاعات شاپرک» الزامی است.

۵-۲-۴-۸- به منظور جلوگیری از نفوذ به درگاه پرداخت اینترنتی، رعایت الزامات جلوگیری از نفوذ و تجهیزات امنیت اطلاعات چند لایه مطابق با سند «الزامات امنیت اطلاعات شاپرک» الزامی است.

۵-۲-۴-۹- در تولید و توسعه صفحه پرداخت اینترنتی، رعایت الزامات امنیت نرم‌افزار تولید داخل سازمان مطابق با سند «الزامات امنیت اطلاعات شاپرک» الزامی است.

۵-۲-۴-۱۰- به منظور تأمین امنیت صفحه پرداخت اینترنتی، رعایت موارد امنیت صفحه پرداخت اینترنتی مطابق با سندهای «الزامات امنیت اطلاعات شاپرک» و «الزامات تولید فایل درخواست جهت صدور گواهی امنیتی» الزامی است.

۵-۲-۴-۱۱- شرکت ارائه‌دهنده خدمات پرداخت، مطابق با سند «الزامات امنیت اطلاعات شاپرک»، نباید از نرم‌افزارهای آماده عمومی از جمله و نه محدود به سیستم‌های متن‌باز مدیریت محتوا برای ارائه سرویس پرداخت اینترنتی استفاده نماید.

۵-۲-۴-۱۲- اطلاعات کارت یا تراکنش باید پس از هر بار به‌روزآوری[۳۳] صفحه پرداخت، پاک شده و درصورت نیاز مجدداً توسط کاربر وارد گردد.

۵-۲-۴-۱۳- در صورت ذخیره سازی PAN، باید تمامی الزامات نگهداری امن PAN مطابق با سند «الزامات امنیت اطلاعات شاپرک» رعایت گردد.

۵-۲-۴-۱۴- شرکت ارائه دهنده خدمات پرداخت پیش از ذخیره‌سازی PAN در هر یک از درگاه‌های مجازی (اعم از درگاه پرداخت اینترنتی، برنامه کاربردی موبایلی و غیره)، باید از دارنده کارت اجازه لازم جهت ذخیره‌سازی شماره کارت را دریافت نماید.

۵-۲-۴-۱۵- شرکت ارائه دهنده خدمات پرداخت مجاز به نمایش PAN در درگاه‌هایی که اجازه لازم بابت ذخیره PAN را از دارنده کارت کسب نکرده است نمی‌باشد. به عبارتی چنانچه دارنده کارت در درگاه پرداخت اینترنتی اجازه ذخیره PAN را به شرکت ارائه دهنده خدمات پرداخت ارائه نموده باشد، شرکت ارائه دهنده خدمات پرداخت مجاز به نمایش PAN در برنامه کاربردی موبایلی نمی‌باشد، مگر این‌که مجوز ذخیره PAN در برنامه کاربردی موبایلی را نیز از دارنده کارت کسب نماید.

---

[۳۲] Referer

[۳۳] Refresh

۵-۲-۴-۱۶- شرکت ارائه دهنده خدمات پرداخت باید امکان حذف PAN یا PANهای ذخیره شده بر روی درگاه‌هایی که قبلاً با اجازه کاربر PAN را بر روی آن‌ها ذخیره نموده است، برای دارنده کارت فراهم نماید.

۵-۲-۴-۱۷- در صورتی که شرکت ارائه‌دهنده خدمات پرداخت دارای چند سرور صفحه پرداخت در شبکه خود باشد، تمامی صفحات پرداخت اینترنتی باید از نظر ظاهر و اطلاعات نمایش داده شده همسان باشند.

۵-۲-۴-۱۸- ارائه سرویس پرداخت اینترنتی تنها تحت دامنه رسمی شرکت شاپرک مجاز است.

۵-۲-۴-۱۹- نمایش لوگوی شرکت شاپرک و شرکت ارائه‌دهنده خدمات پرداخت در صفحه پرداخت باید مطابق با الزامات مندرج در سند «مقررات استفاده از نام و نشان تجاری شاپرک» باشد.

۵-۲-۴-۲۰- مهلت انجام هر تراکنش توسط کاربر، باید با یک زمان‌سنج[۳۴] در صفحه پرداخت نمایش داده شود. این زمان نباید بیشتر از ۱۵ دقیقه باشد. مهلت ورود رمز پویا توسط کاربر ۱۲۰ ثانیه بوده که این زمان به ازای هر درخواست رمز، از نو محاسبه می‌شود.

۵-۲-۴-۲۱- اطلاعات تماس پشتیبانی/ امداد مشتریان شرکت ارائه‌دهنده خدمات پرداخت باید در پایین صفحه پرداخت نمایش داده شود.

۵-۲-۴-۲۲- در مورد تمامی الگوریتم‌های رمزنگاری و پروتکل‌های مورد استفاده درگاه پرداخت، الزامات رمزنگاری قوی مطابق با سند «الزامات امنیت اطلاعات شاپرک» باید رعایت شود.

۵-۲-۴-۲۳- نمایش پیغام‌های خطا به دارنده کارت باید به گونه‌ای صورت پذیرد که اطلاعات حساس کارت و دیگر اطلاعات محرمانه سیستم را برای مهاجم احتمالی افشا نکند.

۵-۲-۴-۲۴- شرکت ارائه‌دهنده خدمات پرداخت باید مستند چگونگی مدیریت انواع خطا، مابین درگاه پرداخت اینترنتی و پذیرنده را تهیه نماید. این مستند باید تمامی انواع خطاها و چگونگی مدیریت هرکدام را شامل شود.

۵-۲-۴-۲۵- ارسال داده‌های اضافی در صفحه پرداخت به صورت پنهان، غیرمجاز می‌باشد.

۵-۲-۴-۲۶- شرکت ارائه‌دهنده خدمات پرداخت باید با رعایت الزامات رمزنگاری قوی مطابق با سند «الزامات امنیت اطلاعات شاپرک»، با استفاده از الگوریتم‌های درهم ساز (Hash)، امضای دیجیتال و غیره، صحت پارامترهای تبادلی با ابزار پذیرش را کنترل نماید.

۵-۲-۴-۲۷- استفاده از لینک، لاگین یا هرگونه ارجاع به صفحه دیگر غیرمجاز می‌باشد. هرگونه فرم، صفحه یا پنجره که به منظور دریافت نام کاربری، رمز عبور یا اطلاعات دیگر، جهت دسترسی به مجموعه‌ای از خدمات، به کاربر نمایش داده شود، لاگین تلقی می‌شود.

۵-۲-۴-۲۸- صفحه پرداخت تنها مجاز به دریافت اطلاعات، به ترتیب زیر می‌باشد:

۱. شماره کارت
۲. شماره شناسایی دوم (CVV2)
۳. تاریخ انقضا
۴. کانال ارسال رمز پویا (پیام کوتاه، ایمیل، برنامک، تماس)

---

[۳۴] Timer

۵. پست الکترونیک دارنده کارت

۶. شماره تلفن همراه دارنده کارت

۷. کپچا (CAPTCHA)

پس از وارد کردن اطلاعات بالا توسط دارنده کارت و ارسال رمز پویا توسط بانک برای دارنده کارت، می‌بایست در همان صفحه از وی «**رمز پویا**» را دریافت نمود.

۸. رمز پویا

لازم به ذکر است پس از درخواست ارسال رمز پویا توسط دارنده کارت، نباید امکان تغییر اطلاعات وارد شده برای دارنده کارت وجود داشته باشد.

دریافت هرگونه اطلاعات به غیر از موارد فوق، مگر با اخذ مجوز از شاپرک، غیرمجاز می‌باشد.

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

۵-۲-۴-۲۹- لازم است فرآیند درخواست رمز دوم یکبار مصرف پس از اطمینان از صحت کپچا (CAPTCHA) وارد شده توسط کاربر انجام گیرد.

۵-۲-۴-۳۰- کاربر می‌تواند در صفحه پرداخت اینترنتی، حداکثر ۵ بار درخواست تولید رمز نماید.

۵-۲-۴-۳۱- کاربر تنها باید با سه کلید «درخواست رمز یکبار مصرف»، «پرداخت» و «انصراف» هدایت لازم را دریافت نماید و حضور کلیدهای اضافی غیرمجاز می‌باشد.

۵-۲-۴-۳۲- سنجش آسیب‌پذیری صفحه پرداخت باید مطابق با الزام سنجش آسیب‌پذیری از سند «الزامات امنیت اطلاعات شاپرک» انجام گیرد.

۵-۲-۴-۳۳- به‌کارگیری پروتکل‌های رمزنگاری امن مطابق با سند «الزامات امنیت اطلاعات شاپرک»، جهت پیشگیری از افشای اطلاعات تبادلی بر روی اینترنت و دیگر بسترهای عمومی الزامی است.

۵-۲-۴-۳۴- اطلاعات قابل نمایش در رسید پذیرندگان اینترنتی، باید در انطباق کامل با الزامات مندرج در سند «مقررات صدور رسیدهای الکترونیکی در پرداخت‌های الکترونیکی مبتنی بر کارت» باشد.

۵-۲-۴-۳۵- شرکت ارائه‌دهنده خدمات پرداخت باید مستندی تحت عنوان «راهنمای انجام تراکنش اینترنتی» را در درگاه پرداخت خود برای دسترسی عموم تهیه و ارائه نماید.

۵-۲-۴-۳۶- شرکت ارائه دهنده خدمات پرداخت باید ترتیبی اتخاذ نماید تا در صفحه پرداخت اینترنتی، اطلاعات زیر به دارنده کارت نمایش داده شود:

- نام فروشگاه
- کد پذیرنده
- کد ترمینال
- مبلغ تراکنش
- آدرس وب‌سایت پذیرنده اینترنتی (URL)

در تراکنش‌های پرداخت‌یاری اطلاعات مجاز جهت نمایش به دارنده کارت به شرح زیر می‌باشد:

- نام و یا لوگوی شرکت پرداخت‌یار
- کد پذیرنده پشتیبانی‌شده
- کد ترمینال پذیرنده پشتیبانی شده
- نام فروشگاه پذیرنده پشتیبانی شده
- مبلغ تراکنش

۵-۲-۴-۳۷- ارسال اطلاعات کارت و اقلام تراکنش صرفاً بر روی ابزارهای پذیرش شرکت ارائه‌دهنده خدمات پرداخت مجاز بوده و ارسال این اطلاعات از طریق وب‌سرویس و دیگر تکنولوژی‌های ارتباطی غیرمجاز می‌باشد.