مجموعه استانداردهای امنیتی پرداخت الکترونیک

PCI

استاندارد پرداخت یوروپی، مسترکارت، ویزا

EMV

پیش‌گفتار

به منظور تقویت و افزایش امنیت اطلاعات دارنده کارت و ایجاد سازگاری با معیارهای جهانی امنیت اطلاعات و با عنایت به وضعیت شبکه بانکی و پرداخت کشور در دوران پساتحریم و لزوم اتصال به شبکه‌های بین‌المللی، یکی از مهم‌ترین پیش نیازها در استقرار فرایندها، محصولات و سامانه‌های کارت‌های اعتباری و هوشمند از قبیل Visa و MasterCard در ایران، آشنایی و پیاده سازی الزامات و استانداردهای فنی بین‌المللی است.

یکی از استانداردهای مهم و اساسی در این زمینه استاندارد EMV است که توسط سه شرکت مطرح دنیا Europay، MasterCard و Visa ارائه شده و هدف آن امکان به‌کارگیری یک کارت در تمام نقاط جهان و کاهش احتمال وقوع هرگونه سوء استفاده و کلاه‌برداری است.

شاید تا پیش از سال ۲۰۱۵ که ایالات متحده تصمیم قطعی مهاجرت به EMV را اتخاذ نکرده بود، جدیت کافی در سطح بین‌المللی برای مهاجرت به EMV وجود نداشت، اما امروزه یکی از مهم‌ترین پروژه‌های بین‌المللی بانک‌ها و شرکت‌های پرداخت مهاجرت سوییچ‌ها، کارت‌ها، ابزارهای پرداخت و زیرساخت‌ها به EMV است.EMV به معنای افزایش امنیت بسترهای پرداخت و کاهش تقلب حوزه کارت است و در عین حال افزایش امکان خدمات نوین در ابزارها و بسترهای جدید که نوید نسلی نو از پرداخت‌های حضوری و غیرحضوری را به همراه دارد.

طبق آمار موجود از کشورهایی که در سالهای گذشته به EMV مهاجرت نموده‌اند، کاهش چشمگیری در تخلفات حوزه کارت صورت گرفته است. به طوری‌که در انگلستان حجم تخلفات کارت‌های مفقوده و مسروقه به پایین‌ترین حد خود در دو دهه اخیر رسیده و ۶۷ درصد از سال ۱۹۹۹ کاهش داشته است و در کانادا از سال ۲۰۰۸ تا ۲۰۱۳ حجم تخلفات کارت از ۱۴۲ میلیون دلار کانادا به ۲۹ میلیون دلار کاهش یافته است.

مجموعه استانداردهای صنعت کارت پرداخت یا PCI نیز با هدف حفظ امنیت اطلاعات کارت پرداخت، تعریف شده و مورد استفاده قرار می‌گیرد. این استاندارد شامل مجموعه‌ای از الزامات امنیتی برای حفظ و نگهداری اطلاعات کارت است و در چهار بخش PCI DSS، PCI PTS، PCI PA-DSS و PCI P2PE ارائه شده است.

به منظور افزایش دانش فنی این حوزه و با توجه به تصمیمات اخیر بانک مرکزی جمهوری اسلامی مبنی بر مهاجرت به EMV، شرکت تجارت الکترونیک پارسیان با همکاری گروه

بانکداری الکترونیک پژوهشکده پولی و بانکی بانک مرکزی اقدام به ترجمه و انتشار مجموعه استانداردهای EMV و PCI برای استفاده نظام بانکی و پرداخت کشور نموده است.

گردآوری و ترجمه: لیلا نامی

معاونت تحقیق و توسعه
شرکت تجارت الکترونیک پارسیان (پککو)
خرداد ۹۵

فهرست مطالب

عنوان **صفحه**

فصل اول

مقدمه.....۱

استاندارد EMV.....۲

استاندارد PCI SSC.....۳

استاندارد امنیت داده PCI DSS.....۴

استاندارد امنیت داده‌های برنامه‌های کاربردی PA-DSS.....۶

امنیت تراکنش احراز هویت PTS.....۷

استاندارد رمزگذاری نقطه به نقطه PCI P2PE.....۱۱

فصل دوم

مقدمه.....۱۳

الزامات و اهداف استاندارد PCI DSS.....۱۴

هدف ۱- ایجاد و حفظ یک شبکه و سیستم امن.....۱۶

هدف ۲- حفاظت از اطلاعات دارنده کارت.....۱۸

هدف ۳- استفاده از برنامه‌های مدیریت آسیب‌پذیری.....۲۱

هدف ۴- اعمال تمهیدات قوی در کنترل دسترسی‌ها.....۲۳

هدف ۵- پایش و ارزیابی مداوم شبکه.....۲۷

هدف ۶- اتخاذ یک سیاست امنیت اطلاعات.....۳۰

مراحل صحت‌سنجی تطبیق با استاندارد PCI DSS.....۳۲

فصل سوم

مقدمه.....۳۹

الزامات استاندارد PA-DSS.....۴۱

الزام ۱.....۴۲

الزام ۲.....۴۵

الزام ۳.....۴۸

الزام ۴.....۵۱

الزام ۵.....۵۳
الزام ۶.....۵۹
الزام ۷.....۶۰
الزام ۸.....۶۱
الزام ۹.....۶۳
الزام ۱۰.....۶۳
الزام ۱۱.....۶۵
الزام ۱۲.....۶۶
الزام ۱۳.....۶۶
الزام ۱۴.....۶۷
الزام ۱۲.....۶۶

فصل چهارم

مقدمه.....**۶۹**
الزامات استاندارد PCI PTS POI.....**۷۴**
ماژول ۱: الزامات اصلی.....۷۶
ماژول ۲: یکپارچه‌سازی پایانه.....۸۳
ماژول ۳: پروتکل‌های باز.....۸۵
ماژول ۴: خواندن و تبادل امن اطلاعات (SRED).....۸۹
ماژول ۵: الزامات امنیتی مدیریت دستگاه.....۹۴
قابلیت‌های پشتیبانی شده توسط دستگاه POI و الزامات مربوطه.....**۹۷**
قابلیت‌های دستگاه POI.....۹۷
رابطه الزامات با قابلیت‌های دستگاه POI.....۹۸
الزامات استاندارد PCI PTS HSM.....**۱۰۱**
A: الزامات امنیتی فیزیکی.....۱۰۲
B: الزامات امنیتی منطقی.....۱۰۳
C: سیاست و روش‌ها.....۱۰۶
D: الزامات امنیتی دستگاه در طول ساخت.....۱۰۷

E: الزامات امنیتی دستگاه بین ساخت و مرکز استقرار اولیه.....۱۰۸
فصل پنجم
مقدمه.....۱۱۱
حوزه‌ها و الزامات استاندارد P2PE.....۱۱۵
حوزه‌های P2PE.....۱۱۵
کاربرد حوزه‌ها برای ارزیابی دستگاه SCD.....۱۱۵
ارتباط حوزه‌ها با نهادهای ارائه‌دهنده خدمات P2PE.....۱۱۶
دامنه ارزیابی راهکارهای P2PE.....۱۱۷
ارتباط میان P2PE و سایر استانداردهای PCI.....۱۱۹
پیاده‌سازی P2PE در یک نگاه.....۱۱۹
الزامات حوزه ۱: مدیریت دستگاه و برنامه کاربردی رمزگذاری.....۱۲۰
الزامات حوزه ۲: امنیت برنامه کاربردی.....۱۲۲
الزامات حوزه ۳: مدیریت راهکار P2PE.....۱۲۳
الزامات حوزه ۴: راهکار مدیریت‌شده توسط پذیرنده.....۱۲۴
الزامات حوزه ۵: محیط رمزگشایی.....۱۲۵
الزامات حوزه ۶: مدیریت عملیات و دستگاه کلید رمزگذاری P2PE.....۱۲۷
فصل ششم
مقدمه.....۱۳۳
هدف.....۱۳۳
EMV چیست.....۱۳۳
مزایای EMV.....۱۳۵
تاریخچه EMV.....۱۳۶
تفاوت EMVCo و سیستم‌های پرداخت بین المللی.....۱۴۰
ارتباط EMVCo با سایر استانداردها.....۱۴۱
مراحل تراکنش و ویژگی‌های EMV.....۱۴۳
تفاوت نوار مغناطیسی و تراشه.....۱۴۳
ویژگی‌های EMV.....۱۴۸

تست و تأییدیه EMV.....**۱۵۵**
هدف کلیدی EMVCo.....۱۵۵
تایید نوع پایانه.....۱۵۵
تایید نوع کارت.....۱۵۶
ارزیابی امنیت تراشه.....۱۵۶
نکات پیاده‌سازی.....**۱۵۶**
نکات صادرکنندگی.....۱۵۷
نکات پذیرندگی و خرده‌فروشی.....۱۵۹

پیوست ۱.....**۱۶۳**
منابع.....**۱۶۹**

فهرست اشکال

عنوان **صفحه**

شکل ۱-۱: اکوسیستم دستگاه‌ها، برنامه‌های کاربردی، زیرساخت و کاربران پرداخت.....۴
شکل ۲-۱: انواع داده روی کارت پرداخت.....۱۴
شکل ۲-۲: روتر و فایروال.....۱۶
شکل ۲-۳: اجزای شبکه.....۳۲
شکل ۲-۴: مراحل انطباق.....۳۳
شکل ۴-۱: نسخه‌های استاندارد PCI PTS.....۷۳
شکل ۴-۲: دستگاه‌های PTS.....۷۳
شکل ۵-۱: پیاده‌سازی PE۲P در یک نگاه.....۱۲۰
شکل ۵-۲: جداسازی محیط رمزگذاری و رمزگشایی پذیرنده.....۱۲۴
شکل ۵-۳: پیاده‌سازی رمزگشایی ترکیبی PE۲P.....۱۲۶
شکل ۶-۱: سیر زمانی EMV.....۱۳۷
شکل ۶-۲: CCD.....۱۳۸
شکل ۶-۳: NFC و غیرتماسی.....۱۳۹
شکل ۶-۴: ارتباط EMVCo با سایر استانداردها.....۱۴۳
شکل ۶-۵: فرآیند تراکنش کارت مغناطیسی.....۱۴۴
شکل ۶-۶: فرآیند تراکنش کارت EMV.....۱۴۵
شکل ۶-۷: مراحل تراکنش تماسی EMV.....۱۴۶
شکل ۶-۸: رمز برنامه کاربردی.....۱۴۹
شکل ۶-۹: مدیریت ریسک و دستورات اسکریپتی.....۱۵۱
شکل ۶-۱۰: پردازش تأیید دارنده کارت.....۱۵۲
شکل ۶-۱۱: احراز هویت داده آفلاین.....۱۵۳
شکل ۶-۱۲: فعالیت‌های پیاده سازی EMV صادرکننده.....۱۵۷
شکل ۶-۱۳: فعالیت‌های پیاده سازی EMV پذیرنده.....۱۵۹

فهرست جداول

عنوان **صفحه**

جدول ۱-۱: اهداف و الزامات استاندارد PCI DSS در یک نگاه.....۵
جدول ۱-۲: الزامات استاندارد PA-DSS در یک نگاه.....۷
جدول ۲-۱: اهداف و الزامات استاندارد PCI DSS.....۱۵
جدول ۲-۲: دستورالعمل المان‌های اطلاعات دارنده کارت.....۲۰
جدول ۲-۳: میزان شدت اسکن آسیب‌پذیری.....۲۹
جدول ۳-۱: اطلاعات حساب.....۴۰
جدول ۳-۲: چگونگی ذخیره اطلاعات حساب.....۴۱
جدول ۳-۳: الزامات استاندارد PA-DSS.....۴۲
جدول ۴-۱: الزامات PCI PTS POI.....۷۴
جدول ۴-۲: موارد ارزیابی در ماژول‌های الزامات اصلی و یکپارچه‌سازی.....۷۵
جدول ۴-۳: موارد ارزیابی در ماژول پروتکل باز.....۷۶
جدول ۴-۴: رابطه الزامات با قابلیت‌های دستگاه POI.....۹۸
جدول ۴-۵: الزامات امنیتی PCI PTS HSM.....۱۰۲
جدول ۴-۶: تکنیک ورود انواع کلیدها.....۱۰۵
جدول ۵-۱: حوزه‌های استاندارد PE۲PCI P.....۱۱۵
جدول ۵-۲: کاربرد حوزه‌ها برای ارزیابی دستگاه SCD.....۱۱۶
جدول ۵-۳: ارتباط حوزه‌ها با نهادهای ارائه‌دهنده خدمات PE۲P.....۱۱۷
جدول ۵-۴: دامنه ارزیابی راهکارهای PE۲P.....۱۱۸
جدول ۶-۱: ضریب نفوذ EMV به تفکیک مناطق.....۱۴۰
جدول ۶-۲: تفاوت EMVCo و سیستم‌های پرداخت بین المللی.....۱۴۱
جدول ۶-۳: فعالیت‌های صادرکنندگی EMV.....۱۵۸
جدول ۶-۴: فعالیت‌های پذیرندگی EMV.....۱۶۰
جدول پ-۱: امتیاز فاکتورهای محاسبه پتانسیل حمله.....۱۶۶
جدول پ-۲: ضرایب دسترسی به TOE.....۱۶۷

فصل ۱

الزامات و استانداردهای فنی مورد نیاز جهت اتصال به شبکه های بین المللی

مقدمه

توجه به الزامات و استانداردهای فنی یکی از مهم ترین پیش نیازها در استقرار فرآیندها، محصولات و سامانه‌های کارت‌های اعتباری بین المللی از قبیل Visa و MasterCard در ایران می‌باشد.

یکی از استانداردهای مهم و اساسی در این زمینه استاندارد EMV و نقش PCI DSS در آن می‌باشد. در ادامه توضیح مختصری از استاندارد EMV و الزامات آن و انواع استانداردهای PCI، الزامات آن و چگونگی تطابق با آن مورد بررسی قرار گرفته است.

استانداردهای مذکور با ذکر تمام جزئیات در قالب دستورالعمل به شرح ذیل در ۶ فصل تدوین شده است.

فصل ۱: الزامات و استانداردهای فنی مورد نیاز جهت اتصال به شبکه‌های بین المللی
فصل ۲: استاندارد امنیت داده PCI DSS (Data Security Standards)
فصل ۳: استاندارد امنیت داده‌های برنامه‌های کاربردی PCI PA_DSS
(Payment Application – Data Security Standard)
فصل ۴: امنیت تراکنش احراز هویت PCI PTS (PIN Transaction Security)
فصل ۵: استاندارد رمزگذاری نقطه به نقطه PCI P2PE (Point-to-Point Encryption)
فصل ۶: استاندارد EMV (Europay, MasterCard, Visa)

استاندارد EMV (Europay, MasterCard, Visa)

مخفف سه کلمه Europay, MasterCard, Visa بوده و برای عملیات بین کارت‌های هوشمند، دستگاه‌های پایانه فروش قادر به پذیرش کارت هوشمند، دستگاه‌های خودپرداز و همچنین تایید تراکنش‌های کارت نقدی و اعتباری می‌باشد. در این استاندارد از روش‌های احراز هویت کارت به همراه PIN و پیشگیری از حملات شبیه‌سازی کارت استفاده می‌شود.

هدف از طراحی کارت هوشمند EMV کاهش احتمال وقوع هرگونه سوء استفاده و کلاه برداری از طریق نوار مغناطیسی می‌باشد.

از آنجا که سرویس‌دهندگان بسیاری در سطح جهان خدمات بانکی مرتبط با کارت هوشمند را ارایه می‌کنند، در صورتی که هر یک بخواهند از سیستم خاص خود استفاده کنند، امکان اتصال این سیستم‌ها به یکدیگر بسیار مشکل می‌گردد. از این رو شرکت‌های مطرح در این زمینه (Visa, Europay, MasterCard) اقدام به ارایه یک استاندارد واحد با نام EMV در این زمینه نموده‌اند. هدف اصلی از ارایه این استاندارد، امکان بکارگیری یک کارت در تمام نقاط جهان می‌باشد.

ارتباط و الزامات EMV با سایر استانداردها:

۱) International Organisation for Standardisation (ISO):

- ISO/IEC 7816: Identification Cards – Integrated Circuit(s) Cards
- ISO/IEC 14443: Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards

۲) Payment Card Industry Security Standards Council (PCI SSC):

در درجه اول از اطلاعات حساس پرداخت مانند اطلاعات حساب و شماره شناسایی شخصی (PIN) حفاظت می‌کند. EMV و PCI در افزایش امنیت پرداخت و کاهش تقلب در کارت‌های جعلی و مفقودی و به سرقت رفته مکمل هم می‌باشند. EMV قادر به حفاظت از اطلاعات کلیدی و جلوگیری از عناصر داده‌های حیاتی تراکنش نیست. بنابراین وجود استاندارد PCI DSS امری ضروری است.

۳) The Near Field Communication (NFC) Forum:

بیشتر پرداخت‌های EMV از کانال‌های موبایل و غیرتماسی می‌باشد. بنابراین هماهنگی با NFC Forum جهت توسعه مشخصات اتصال میان دستگاه‌ها و خدمات NFC موردنیاز است.

۴) GlobalPlatform:

بخشی از فعالیت‌های EMV بررسی عملکرد و امنیت پلتفرمی است که برنامه پرداخت EMV بر روی آن مستقر می‌شود. جهت حمایت از برنامه‌های متعدد، از منابع مختلف نیاز به هماهنگی با استانداردهای GlobalPlatform می‌باشد.

استاندارد PCI SSC

(Payment Card Industry Security Standards Council)

PCI (Payment Card Industry) استاندارد بین‌المللی است که با هدف حفظ امنیت اطلاعات کارت پرداخت، تعریف شده و مورد استفاده قرار می‌گیرد. این استاندارد شامل مجموعه‌ای از الزامات امنیتی برای حفظ و نگهداری اطلاعات کارت است. اعضاء، پذیرندگان وPSP ها بایستی قوانین آن را رعایت نمایند. از سال ۲۰۰۶ کمیته‌ای برای پیاده‌سازی، نگهداری و مدیریت استانداردهای امنیتی PCI شروع به فعالیت نموده است.

اعضای موسس این استاندارد شرکتهای American Express، Discover Financial Services، JCB، MasterCard و Visa Inc می‌باشند. این فعالیت‌ها در چهار بخش اصلی به شرح ذیل انجام می‌گیرد:

۱) PCI DSS (PCI Data Security Standard)
۲) PCI PTS (PIN Transaction Security) requirements
۳) PCI PA-DSS (Payment Application Data Security Standard)
۴) PCI P2PE (Point-to-Point Encryption) Standard

شکل ۱-۱: اکوسیستم دستگاه‌ها، برنامه‌های کاربردی، زیرساخت و کاربران پرداخت

۱) استاندارد امنیت داده (PCI DSS (PCI Data Security Standard

استاندارد ایمنی داده صنعت کارت پرداخت و استاندارد امنیت اطلاعات می‌باشد که برای سازمان‌هایی که با اطلاعات دارندگان کارت‌های دستگاه پایانه فروش، خودپرداز، کیف پول الکترونیک (e-purse)، پیش پرداخت شده (prepaid)، اعتباری و نقدی سروکار دارند طراحی شده است. این استاندارد دارای ۶ هدف و ۱۲ الزام جهت رسیدن به آن اهداف می‌باشد:

جدول ۱-۱: اهداف و الزامات استاندارد PCI DSS در یک نگاه

اهداف	الزامات PCI DSS
هدف ۱: ایجاد و حفظ یک شبکه و سیستم امن	**الزام ۱:** نصب سیستم‌های Firewall جهت حفاظت از اطلاعات مربوط به دارندگان کارت‌های پرداخت الکترونیک **الزام ۲:** عدم استفاده از تنظیمات پیش فرض انجام شده توسط فروشندگان و سازندگان تجهیزات، مانند رمز عبور و دیگر پارامترهای امنیتی
هدف ۲: حفاظت از اطلاعات دارنده کارت	**الزام ۳:** محافظت از داده‌های ذخیره شده مربوط به دارندگان کارت‌ها **الزام ۴:** رمزنگاری نقل و انتقال اطلاعات دارندگان کارت‌ها در شبکه‌های باز و عمومی
هدف ۳: استفاده از برنامه‌های مدیریت آسیب پذیری	**الزام ۵:** حفاظت از کل سیستم در برابر بدافزارها ونصب نرم‌افزار Antivirusو به روز رسانی مداوم آن **الزام ۶:** توسعه و نگهداری سیستم‌های ایمن و برنامه‌های کاربردی امن
هدف ٤: اعمال تمهیدات قوی در کنترل دسترسی‌ها	**الزام ۷:** محدود کردن دسترسی به اطلاعات دارندگان کارت‌ها در حداقل احتیاج هر کسب و کار **الزام ۸:** شناسایی و احراز هویت دسترسی به اجزای سیستم **الزام ۹:** محدود کردن دسترسی فیزیکی به اطلاعات دارندگان کارت‌ها
هدف ٥: پایش و ارزیابی مداوم شبکه	**الزام ۱۰:** پایش و ردیابی مداوم هرگونه دسترسی به منابع اطلاعاتی، تجهیزات شبکه و همچنین اطلاعات مربوط به دارندگان کارت‌ها **الزام ۱۱:** ارزیابی منظم و قاعده مند امنیت سیستم‌ها و فرآیندهای امنیتی لحاظ شده
هدف ٦: اتخاذ یک سیاست امنیت اطلاعات	**الزام ۱۲:** سیاستی اتخاذ شود که خط مشی‌های امنیت اطلاعات در آن برای تمام پرسنل مشخص گردد

۲) استاندارد امنیت داده‌های برنامه‌های کاربردی PA-DSS (Payment Application-Data Security Standard)

PA-DSS مخفف Payment Application – Data Security Standard و استاندارد امنیت داده‌های برنامه‌های کاربردی پرداخت بوده و در راستای حفظ امنیت داده‌ها در نرم‌افزارهای کاربردی لازم است که این برنامه‌ها عملیات ذخیره‌سازی و پردازش و انتقال دو گونه داده شامل داده‌های دارنده کارت (مانند نام دارنده کارت و PAN) و داده‌های احراز هویت (مانند اطلاعات شیار ۲ و CVV2) کارت پرداخت را با پشتیبانی از استاندارد PA-DSS انجام دهند.

رعایت این استاندارد در محدوده زیر تعریف می شود:

- توابع و اجزاء پرداخت (End-to-End)
- ورودی و خروجی
- شرایط خطا
- رابط‌های کاربر و ارتباط با سایر سیستم‌ها، فایل‌ها، برنامه‌های پرداختی
- جریان داده‌های دارنده کارت
- مکانیزم‌های رمزنگاری
- مکانیزم‌های احراز هویت

این استاندارد ۱۴ الزام برنامه‌های کاربردی پرداخت برای هر کسب و کاری، اعم از فروشندگان نرم‌افزار، شرکت‌های ارایه‌دهنده خدمات پرداخت، بانک‌ها و مشتریان در نظر گرفته است که این الزامات، یک چارچوب کاری برای محیط امن برنامه کاربردی پرداخت را تعریف می‌کند. این الزامات، عبارتند از:

جدول ۱-۲: الزامات استاندارد PA-DSS در یک نگاه

الزامات PA-DSS
الزام ۱: اطلاعات کامل، از جمله کد یا مقدار امنیتی کارت (CAV2[1]، CID[2]، CVC2[3]، CVV2[4])، و یا اطلاعات PIN block نگهداری نشود.
الزام ۲: از اطلاعات ذخیره شده دارنده کارت محافظت گردد.
الزام ۳: ویژگی‌های احراز هویت امن ارائه شود.
الزام ۴: فعالیت‌های برنامه کاربردی پرداخت ثبت گردد.
الزام ۵: برنامه‌های کاربردی پرداخت امن ایجاد شود.
الزام ۶: از انتقال بی سیم محافظت شود.
الزام ۷: برنامه‌های کاربردی پرداخت جهت شناسایی آسیب پذیری‌ها تست و آپدیت شود.
الزام ۸: پیاده سازی شبکه امن تسهیل شود.
الزام ۹: اطلاعات دارنده کارت نباید هرگز در سرور متصل به اینترنت ذخیره شود.
الزام ۱۰: دسترسی امن از راه دور به برنامه کاربردی پرداخت تسهیل شود.
الزام ۱۱: ترافیک حساس بر روی شبکه‌های عمومی رمزگذاری گردد.
الزام ۱۲: تمام دسترسی‌های مدیریتی غیرکنسول رمزگذاری شود.
الزام ۱۳: الزامات پیاده سازی PA-DSS برای مشتریان، فروشندگان و یکپارچه سازان ارائه شود.
الزام ۱۴: مسئولیت‌های PA-DSS برای پرسنل اختصاص یافته، و برنامه‌های آموزشی برای پرسنل، مشتریان، نمایندگان فروش و یکپارچه سازان ارائه گردد.

۳) امنیت تراکنش احراز هویت PTS (PIN Transaction Security)

[1] Card Authentication Value
[2] Card Identification Number
[3] Card Verification Code
[4] Card Verification Value

این بخش از استاندارد از اولویت‌های استراتژیک PCI محسوب می شود و هدف اصلی آن حفاظت از PIN می‌باشد.

در این خصوص سه نوع دستگاه موردنظر می‌باشد:

- **PED (PIN Entry Device)** ، شامل انواع ترمینال‌هایی که توسط پذیرنده‌ها جهت تراکنش‌های کارت استفاده می‌گردد.
- **EPP (Encrypting PIN PAD)** ، بخشی از پایانه‌ها از نوع غیر حضوری مانند ATM (Automated Teller Machine) که جهت ورود از رمز استفاده می گردد.
- اجزاء امن پایانه‌های فروش مانند کارتخوان‌های امن و دستگاه‌های مربوط به ورود رمز دارنده کارت می‌باشد.

در PTS خصوصیات فیزیکی و قابلیت دستگاه‌های ورود رمز دارنده کارت مشخص شده است.

در این استاندارد نیازمندی‌های این تجهیزات و داده‌های لازم برای این استاندارد، روش تست و مراحل دریافت و تاییدیه تعریف شده است. بر اساس این مشخصات، دستگاه می‌بایست نفوذ فیزیکی (attack) و نفوذ برای دستیابی به کلیدهای ذخیره شده در دستگاه را تشخیص دهد.

این مهم در کل چرخه حیات دستگاه از تولید تا بکارگیری آن می بایست قابل کنترل باشد و به خوبی مدیریت گردد.

وجود این استاندارد باعث تسریع در توسعه فناوری پرداخت شده است. در گذشته فروشندگان این گونه تجهیزات نیاز به انجام تست‌های اختصاصی در آزمایشگاه‌ها داشتند که وقت‌گیر و پرهزینه بوده است. اما با ایجاد استانداردهای امنیتی بین‌المللی قدم موثری در کاهش هزینه و پیچیدگی‌های تراکنش‌های پرداخت کارت برداشته شده است.

از جمله شرکت‌های معتبری که در کمیته طراحان این استاندارد فعالیت داشته‌اند JCB ، VISA و Mastercard می‌باشند.

در این استاندارد امنیت PIN با ترکیبی از امنیت فیزیکی و منطقی تامین خواهد شد.

پایانه‌ها از نظر فیزیکی می‌بایست ویژگی‌های زیر را داشته باشند:

- Tamper detection: این دستگاه‌ها از مکانیزم‌هایی مانند Secure box، Zebra connector جهت تشخیص Tampering استفاده می کنند.
- با تشخیص دستکاری دستگاه، کلیه اطلاعات مربوط به کلیدهای بارگذاری شده آن حذف گردد.
- Tamper evidence: این دستگاه‌ها با نمایش وضعیت Tampering اجازه انجام عملیات را نمی‌دهند.
- تنها با ابزارهایی خاص امکان برگرداندن این دستگاه‌ها به حالت عملیاتی وجود خواهد داشت.

پایانه‌ها از نظر منطقی می بایست ویژگی‌های زیر را داشته باشند:

- هر نرم‌افزاری که بر امنیت اثرگذار می‌باشد لازم است قبل از بارگذاری، احراز هویت شود.
- رابط‌های کاربری برای ورود رمز می‌بایست کاملا واضح باشند و باعث سردرگمی مشتری نگردد. لذا در برخی پایانه‌ها این بخش از نرم‌افزار می بایست احراز هویت گردند.
- پایانه می‌بایست ازالگوریتم‌های رمزنگاری برای احرازهویت به صورت online پشتیبانی نماید.
- پایانه می‌بایست از متدهای پروتکل EMV برای احراز هویت به صورت offline پشتیبانی نماید.

مدیریت PIN :

نیازهای امنیتی در ورود رمز کارت:

- وجود حفاظ برای مخفی نگاهداشتن کلیدهای وارد شده در پایانه.
- راهنمایی صحیح و واضح به مشتری هنگام ورود رمز کارت.

- حفاظت در مقابل پایش صوت، تشعشعات الکترومغناطیس و مصرف برق برای کشف رمز کارت.
- سازگاری با استاندارد ISO 9564-1، این استاندارد حداقل نیازمندی‌ها را در online PIN بیان می‌کند.

انواع روش‌های صحت رمز مشتری:

- Online PIN verification:

در این روش صحت شماره رمز مشتری به صورت online و توسط سوییچ کارت کنترل می‌گردد که مرتبط با کارت‌های مغناطیسی و هوشمند می‌باشد.

نحوه انتقال رمز و محدودیت‌های مورد نیاز به شرح ذیل می‌باشد:

- ✓ استفاده از کلیدهای متقارن با الگوریتم‌های DES/3DES در تولید کلید Session
- ✓ استفاده از کلیدهای متقارن DES و 3DES در روش DUKPT (Drive Unique Key Per Transaction)
- ✓ بارگذاری کلید به صورت امن
- ✓ عدم تشابه کلیدها
- ✓ عدم دسترسی برنامه به رمز وارد شده توسط مشتری
- ✓ پشتیبانی از استاندارد ISO 9564-2، در این استاندارد الگوریتم‌های رمزنگاری PIN (Personal Identification Number) تعریف شده است.

- Offline PIN verification:

در این روش صحت شماره رمز مشتری به صورت offline توسط کارت هوشمند کنترل می‌گردد. تبادل کلید بین پایانه و کارت به صورت‌های زیر می تواند باشد:

- ✓ بررسی صحت شماره رمز با ارسال PIN وارد شده به کارت
- ✓ بررسی صحت شماره رمز با ارسال PIN رمز شده به کارت
- ✓ استفاده از تولید کننده شماره تصادفی مطابق با NIST 800-22

- ✓ عدم دسترسی برنامه به رمز وارد شده توسط مشتری
  - رمز باید در PED وارد شده باشد
  - PIN برای کنترل به کارت ارسال گرددپایه و اساس کار این استاندارد افزایش کنترل‌ها روی داده می باشد و در تمام بخش‌هایی که اطلاعات دارنده کارت را نگهداری و پردازش و تبادل می‌کنند، قابل استفاده است.

۴) استاندارد رمزگذاری نقطه به نقطه PCI P2PE (Point-to-Point Encryption) Standard

استاندارد رمزگذاری نقطه به نقطه (P2PE) مجموعه‌ای جامع از نیازمندی‌های امنیتی را برای ارائه‌دهندگان راهکار P2PE جهت اعتباربخشی به راهکار P2PE خود و کاهش دامنه PCI DSS فراهم می‌کند. P2PE یک برنامه عملکرد متقابل در استاندارد PTS، PA-DSS، PCI DSS و استاندارد امنیت PCI PIN است.

فصل ۲

استاندارد امنیت داده PCI DSS (Data Security Standards)

مقدمه

PCI DSS مجموعه جامعی از قوانین است که برای ارتقاء سیستم امنیتی داده‌های مربوط به صنعت کارت‌های پرداخت وضع گردیده و هدف آن، کمک جهت تسهیل روند اتخاذ تمهیدات امنیتی مربوط به داده‌های پایدار در یک جامعه جهانی است. این استاندارد، توسط مؤسسین سیستم پرداخت برندهای تجاری شورای استانداردهای امنیتی PCI ایجاد شده است که از میان آن‌ها می‌توان به سازمان‌های بزرگ پرداخت الکترونیک همچون American Express، Discover Financial Cervices، JCB Internationalو MasterCard Worldwide Incاشاره نمود.

PCI DSS یک استاندارد امنیت اطلاعات است که هر کسب و کاری با هر حد و اندازه، برای استفاده از کارت‌های پرداخت و همچنین ذخیره سازی، پردازش و یا ارسال

اطلاعات صاحب کارت باید آن را دریافت نماید. بنابراین، اخذ استاندارد امنیت اطلاعات صنعت کارت‌های پرداخت، برای فروشندگانی که از فناوری کارت پرداخت در سیستم فروش خود استفاده می‌کنند و شرکت‌هایی که اطلاعات شخصی دارندگان این نوع کارت را پردازش می‌نمایند، یک موضوع مهم و ضروری می‌باشد.

این استاندارد جامع، در واقع نوعی استاندارد امنیتی چند وجهی است که شامل نیازمندی‌هایی برای مدیریت امنیت، سیاست‌ها، رویه‌ها، معماری شبکه، طراحی نرم‌افزار و دیگر تمهیدات حفاظتی حساس بوده و کمک به بانک‌ها و مؤسسات مالی، جهت حفاظت از داده‌های مربوط به حساب‌های مشتریانشان را به عنوان هدف خود در نظر می‌گیرد.

شکل ۲-۱: انواع داده روی کارت پرداخت

استاندارد PCI DSS با زمینه کاری استاندارد ISO 17799 و ISO 27002 مطابقت داشته و سازمان‌هایی که در زمینه کارت‌های پرداخت فعالیت دارند و استاندارد ISO 17799سیستم مدیریت امنیت اطلاعات (ISMS) را قبلاً اجرا نموده اند با کمترین اقدامات اضافی قادر خواهند بود تا استاندارد PCI DSS را نیز در سازمان خود، به منظور مدیریت بهتر حفاظت اطلاعات پیاده‌سازی نمایند.

الزامات و اهداف استاندارد PCI DSS

این استاندارد در ۶ اصل مشخص، ۱۲ الزام را برای هر کسب و کاری، اعم از فروشندگان، شرکت‌های ارائه‌دهنده خدمات کارت و بانک‌ها که اطلاعات دارندگان کارت‌های پرداخت را ذخیره، پردازش و یا منتقل می‌کنند، در نظر گرفته است که این

ملزومات، یک چارچوب کاری برای محیط امن پرداخت کارتی را تعریف می‌کند. این الزامات، عبارتند از:

جدول ۲-۱: اهداف و الزامات استاندارد PCI DSS

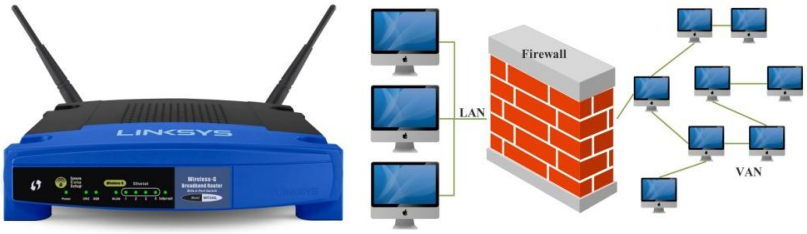
اهداف	الزامات PCI DSS
هدف ۱: ایجاد و حفظ یک شبکه و سیستم امن	**الزام ۱:** نصب سیستم‌های Firewall جهت حفاظت از اطلاعات مربوط به دارندگان کارت‌های پرداخت الکترونیک **الزام ۲:** عدم استفاده از تنظیمات پیش فرض انجام شده توسط فروشندگان و سازندگان تجهیزات، مانند رمز عبور و دیگر پارامترهای امنیتی
هدف ۲: حفاظت از اطلاعات دارنده کارت	**الزام ۳:** محافظت از داده‌های ذخیره شده مربوط به دارندگان کارت‌ها **الزام ۴:** رمزنگاری نقل و انتقال اطلاعات دارندگان کارت‌ها در شبکه‌های باز و عمومی
هدف ۳: استفاده از برنامه‌های مدیریت آسیب‌پذیری	**الزام ۵:** حفاظت از کل سیستم در برابر بدافزارها ونصب نرم‌افزار Antivirusو به روز رسانی مداوم آن **الزام ۶:** توسعه و نگهداری سیستم‌های ایمن و برنامه‌های کاربردی امن
هدف ٤: اعمال تمهیدات قوی در کنترل دسترسی‌ها	**الزام ۷:** محدود کردن دسترسی به اطلاعات دارندگان کارت‌ها در حداقل احتیاج هر کسب و کار **الزام ۸:** شناسایی و احراز هویت دسترسی به اجزای سیستم **الزام ۹:** محدود کردن دسترسی فیزیکی به اطلاعات دارندگان کارت‌ها
هدف ۵: پایش و ارزیابی مداوم شبکه	**الزام ۱۰:** پایش و ردیابی مداوم هرگونه دسترسی به منابع اطلاعاتی، تجهیزات شبکه و همچنین اطلاعات مربوط به دارندگان کارت‌ها **الزام ۱۱:** ارزیابی منظم و قاعده مند امنیت سیستم‌ها و فرآیندهای امنیتی لحاظ شده
هدف ٦: اتخاذ یک سیاست امنیت اطلاعات	**الزام ۱۲:** سیاستی اتخاذ شود که خط مشی‌های امنیت اطلاعات در آن برای تمام پرسنل مشخص گردد

۱) هدف ۱- ایجاد و حفظ یک شبکه و سیستم امن:

در گذشته، سرقت از پرونده‌های مالی نیازمند ورود مجرم به محل سازمان کسب و کار بود. در حال حاضر، بسیاری از تراکنش‌های کارت پرداخت با استفاده از دستگاه‌ها و کامپیوترهای ورود PIN متصل به شبکه انجام می‌گیرد. با استفاده از کنترل امنیت شبکه، می‌توان از دسترسی تقریبی مجرمان به شبکه سیستم پرداخت و سرقت اطلاعات دارنده کارت و / یا داده‌های حساس احراز هویت جلوگیری نمود.

الزام ۱- نصب سیستم‌های Firewall جهت حفاظت از اطلاعات مربوط به دارندگان کارت‌های پرداخت الکترونیک:

فایروال‌ها دستگاه‌هایی هستند که ترافیک داخلی و خارجی شبکه یک سازمان و مناطق حساس در شبکه داخلی آن را کنترل می‌نمایند. روتر سخت افزار یا نرم‌افزاری است که به دو یا چند شبکه متصل است.



شکل ۲-۲: روتر و فایروال

فرآیندها و کنترل‌های امنیتی لازم:

۱-۱: تاسیس و پیاده‌سازی استانداردهای پیکربندی فایروال و روتر جهت رسمی نمودن تست در زمان تغییر تنظیمات صورت پذیرد، به طوری که تمام اتصالات میان محیط اطلاعات دارنده کارت و سایر شبکه‌ها (از جمله بی‌سیم) را همراه با مستندات و نمودارها شناسایی نماید؛ می‌بایست از تنظیمات فنی مختلفی برای هر اجرا استفاده نموده و این

دیاگرام در طول سیستم و شبکه جریان یافته و خلاصه ای از مجموعه قوانین پیکربندی حداقل هر شش ماه یکبار تبیین گردد.

۱-۲: یک پیکربندی فایروال و روتر ایجاد شود تا تمام ترافیک (ورودی و خروجی) شبکه (از جمله بی‌سیم) و میزبان نامطمئن را محدود کرده و به جز پروتکل‌های لازم برای محیط اطلاعات دارنده کارت را رد کند.

۱-۳: از دسترسی عمومی مستقیم میان اینترنت و هر یک از اجزای سیستم در محیط اطلاعات دارنده کارت ممانعت شود.

۱-٤: بر روی تلفن‌های همراه و/یا دستگاه‌های متعلق به کارکنان که از اتصال به اینترنت در خارج از شبکه سازمان برای دسترسی به شبکه سازمان استفاده می‌کند، نرم‌افزار فایروال شخصی نصب شود.

۱-۵: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

الزام ۲- عدم استفاده از تنظیمات پیش فرض انجام شده توسط فروشندگان و سازندگان تجهیزات، مانند رمز عبور و دیگر پارامترهای امنیتی:

ساده ترین راه برای یک هکر برای دسترسی به شبکه داخلی استفاده از کلمات عبور پیش فرض و یا سوء استفاده بر اساس تنظیمات پیش فرض سیستم نرم‌افزار در زیرساخت کارت‌های پرداخت است. اغلب پذیرندگان، کلمه عبور و تنظیمات پیش فرض را تغییر نمی‌دهند. کلمه عبور و تنظیمات پیش فرض بسیاری از دستگاه‌های شبکه کاملا شناخته شده است.

فرآیندها و کنترل‌های امنیتی لازم:

۲-۱: همیشه قبل از نصب یک سیستم در شبکه، تمام پیش فرض‌های فروشنده تغییر داده شود و حساب‌های پیش فرض غیر ضروری حذف و یا غیرفعال گردد. این عمل برای

دستگاه‌های بی‌سیمی است که به محیط اطلاعات دارنده کارت متصل شده و یا برای انتقال اطلاعات دارنده کارت استفاده می‌شود.

۲-۲: استانداردهای پیکربندی برای تمام اجزای سیستم که به آسیب‌پذیری‌های امنیتی شناخته شده و مطابق با تعاریف پذیرفته شده صنعت می‌باشند، توسعه یابد. استانداردهای پیکربندی سیستم برای نسخه‌های جدید شناخته شده آسیب‌پذیری بروزرسانی شود.

۲-۳: دسترسی‌های مدیریتی غیر کنسول مانند ابزار مدیریت مبتنی بر وب/ مرورگر با استفاده از رمزنگاری قوی، رمزگذاری شود.

۲-٤: فهرستی از اجزای سیستم که در حوزه هدف PCI DSS می‌باشند ایجاد گردد.

۲-٥: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

۲-٦: ارائه‌دهندگان خدمات میزبانی به‌اشتراک‌گذاشته‌شده، بایستی محیط و اطلاعات دارنده کارت میزبانی شده هر نهاد را محافظت نماید.

۲) هدف ۲- حفاظت از اطلاعات دارنده کارت:

اطلاعات دارنده کارت اشاره به هر گونه اطلاعات است که چاپ، پردازش، انتقال و یا ذخیره می‌گردد. نهادهای پذیرش کارت‌های پرداخت بایستی برای محافظت از اطلاعات دارنده کارت از استفاده غیر مجاز آن جلوگیری نمایند.

الزام ۳- محافظت از داده‌های ذخیره شده مربوط به دارندگان کارت‌ها:

به طور کلی، اطلاعات دارنده کارت نباید ذخیره گردد مگر اینکه برای پاسخگویی به نیازهای کسب و کار موردنیاز باشد. اطلاعات حساس بر روی نوار مغناطیسی و یا تراشه هرگز نباید ذخیره شود.

فرآیندها و کنترل‌های امنیتی لازم:

۳-۱: ذخیره اطلاعات دارنده کارت و زمان نگهداری آن که برای اهداف کسب و کار، اهداف قانونی و یا نظارتی مورد نیاز می‌باشد، بر طبق سیاست حفظ اطلاعات مستندشده محدود گردد. داده‌های غیر ضروری ذخیره شده حداقل هر سه ماه پاکسازی شود.

۳-۲: اطلاعات حساس احراز هویت بعد از احراز هویت حتی در حالت رمزشده ذخیره نشود. تمام اطلاعات احراز هویت حساس، پس از اتمام فرایند احراز هویت غیرقابل بازیابی باشد. صادر کنندگان و نهادهای مرتبط ممکن است اطلاعات حساس احراز هویت را در صورت وجود توجیه کسب و کاری و ذخیره امن آنها نگهداری کنند.

۳-۳: PAN[1] هنگام نمایش (مثلا در دستگاه POS) پنهان شود. حداکثر تعداد ارقام ممکن جهت نمایش شش رقم اول و چهار رقم آخر آن می‌باشد، به طوری که تنها افراد مجاز با نیاز کسب و کار مشروع می‌توانند PAN کامل را ببینند، مخصوصا در رسید پایانه‌های فروش POS بایستی رعایت شود.

۳-٤: PAN در رسانه‌های قابل حمل دیجیتال، رسانه‌های پشتیبان، logها، و اطلاعات دریافت شده و یا ذخیره شده توسط شبکه‌های بی‌سیم، به صورت ناخوانا ذخیره شود. راهکار تکنولوژی برای این منظور، نیازمند توابع هش یک طرفه قوی، کوتاه سازی، نشانه‌گذاری، پد ذخیره شده و ایمن، و یا رمزنگاری قوی می‌باشد.

۳-۵: روش‌های حفاظت از کلیدهای رمزنگاری مورد استفاده برای رمزگذاری اطلاعات دارنده کارت در برابر افشا و سوء استفاده مستند و اجرا شود.

۳-۶: فرآیندها و روش‌های مدیریت تمام کلیدهای رمزنگاری که برای رمزگذاری اطلاعات دارنده کارت استفاده می‌شود به طور کامل مستند و پیاده‌سازی گردد.

۳-۷: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

[1] Primary Account Number

جدول ۲-۲: دستورالعمل المان‌های اطلاعات دارنده کارت

	نوع اطلاعات	مجوز ذخیره	ذخیره اطلاعات به صورت ناخوانا طبق الزام ۳-۴
اطلاعات دارنده کارت	PAN	دارد	دارد
	نام دارنده کارت	دارد	ندارد
	کد سرویس	دارد	ندارد
	تاریخ انقضا	دارد	ندارد
اطلاعات حساس احراز هویت	اطلاعات کامل مسیر	ندارد	طبق الزام ۳-۲ نمیتواند ذخیره شود
	CAV[1]2 / CVC[2]2 / CVV[3]2 / CID	ندارد	طبق الزام ۳-۲ نمیتواند ذخیره شود
	PIN / PIN Block	ندارد	طبق الزام ۳-۲ نمیتواند ذخیره شود

الزام ۴- رمزنگاری نقل و انتقال اطلاعات دارندگان کارت‌ها در شبکه‌های باز و عمومی:

مجرمان سایبری ممکن است قادر به رهگیری انتقال اطلاعات دارنده کارت از شبکه‌های باز و عمومی باشند، بنابراین جلوگیری از توانایی آنها در مشاهده این اطلاعات بسیار مهم است. تکنولوژی مورد استفاده برای این امر رمزگذاری می‌باشد.

فرآیندها و کنترل‌های امنیتی لازم:

۴-۱: از رمزنگاری و پروتکل‌های امنیت قوی مانند TLS[5] / SSH[4] و یا IPSEC[1] برای حفاظت از اطلاعات حساس دارنده کارت در زمان انتقال در شبکه‌های باز و عمومی (مثلا

[1] Card Authentication Value
[2] Card Verification Code
[3] Card Verification Value
[4] Secure SHell
[5] Transport Layer Security

اینترنت، فن‌آوری‌های بی‌سیم، تکنولوژی سلولی، GPRS[2]، مخابرات ماهواره‌ای) استفاده شود. از Best Practiceهای صنعت (به عنوان مثال، IEEE[3] 802.11i) برای اجرای رمزنگاری قوی برای احراز هویت و انتقال در شبکه‌های بی‌سیم انتقال اطلاعات دارنده کارت و یا اتصال به محیط اطلاعات دارنده کارت استفاده شود. استفاده از WEP[4] به دلیل کنترل امنیتی ممنوع است.

۴-۲: هرگز PAN های رمز نشده با تکنولوژی پیام رسانی کاربران نهایی ارسال نشود. (برای مثال، ایمیل، پیام‌های فوری، اس ام اس، چت، و غیره)

۴-۳: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

۳) هدف ۳- استفاده از برنامه‌های مدیریت آسیب‌پذیری:

مدیریت آسیب‌پذیری روندی سیستماتیک و پیوسته برای پیدا کردن نقاط ضعف در سیستم زیرساخت کارت پرداخت یک نهاد است. مدیریت آسیب‌پذیری شامل روش‌های امنیتی، طراحی سیستم، پیاده‌سازی، و یا کنترل‌های داخلی است که حتی می‌تواند در جهت نقض سیاست‌های امنیتی باشد.

الزام ۵- حفاظت از کل سیستم در برابر بدافزارها ونصب نرم‌افزار Antivirus و به روز رسانی مداوم آن:

بسیاری از آسیب‌پذیری‌ها و ویروس‌های مخرب از طریق ایمیل کارکنان و دیگر فعالیت‌های آنلاین وارد شبکه می‌شوند. نرم‌افزار آنتی ویروس بایستی بر روی تمام سیستم‌های تحت تاثیر نرم‌افزارهای مخرب برای محافظت سیستم از تهدید برنامه‌های مخرب فعلی و در حال تحول مورد استفاده قرار گیرد.

---

[1] Internet Protocol Security
[2] General Packet Radio Service
[3] Institute of Electrical and Electronics Engineers
[4] Wired Equivalent Privacy

فرآیندها و کنترل‌های امنیتی لازم:

۵-۱: نرم‌افزار آنتی ویروس بر روی تمام سیستم‌های تحت تاثیر برنامه‌های مخرب (به خصوص رایانه‌های شخصی و سرور) قرار داده شود. برای سیستم‌هایی که معمولا تحت تاثیر برنامه‌های مخرب نیستند، برای تهدید نرم‌افزارهای مخرب جدید ارزیابی دوره ای انجام شده و تعیین گردد آیا چنین سیستم‌هایی همچنان به نرم‌افزار آنتی ویروس نیاز دارند.

۵-۲: تمام مکانیزم‌های آنتی ویروس بایستی رایج بوده، به طور فعال اجرا گشته و توانایی ایجاد logهای مربوطه را داشته باشد.

۵-۳: مکانیسم‌های ضد ویروس بایستی به طور جدی در حال اجرا باشد و نمی‌تواند غیر فعال شود و یا توسط کاربران تغییر داده شود، مگر اینکه به طور خاص توسط مدیریت و موردی برای یک دوره زمانی محدود مجاز شود.

۵-٤: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

الزام ۶- توسعه و نگهداری سیستم‌های ایمن و برنامه‌های کاربردی امن:

آسیب‌پذیری‌های امنیتی در سیستم‌ها و برنامه‌های کاربردی به مجرمان اجازه دسترسی به PAN و دیگر اطلاعات دارنده کارت را می‌دهد. بسیاری از این آسیب‌پذیری‌ها با نصب patchهای امنیتی فروشنده ارائه می‌شود.

فرآیندها و کنترل‌های امنیتی لازم:

٦-۱: یک فرایند برای شناسایی آسیب‌پذیری‌های امنیتی، با استفاده از منابع معتبر خارجی ایجاد کرده و رتبه بندی خطر به آسیب‌پذیری‌های امنیتی تازه کشف شده اختصاص داده شود (مثلا "بالا"، "متوسط" یا "پایین").

٦-۲: تمام اجزای سیستم و نرم‌افزار با نصب patchهای امنیتی قابل اجرای فروشنده از آسیب‌پذیری‌های شناخته شده محافظت گردد. Patch های امنیتی حیاتی در عرض یک ماه پس از انتشار نصب شود.

۶-۳: برنامه‌های کاربردی نرم‌افزارهای داخلی و خارجی از جمله دسترسی مدیریتی مبتنی بر وب به برنامه‌های کاربردی مطابق با PCI DSS و best practiceهای صنعت توسعه یابد. امنیت اطلاعات در طول چرخه حیات توسعه نرم‌افزار ترکیب شود. این مورد برای همه نرم‌افزارهای داخلی، قرار دادی و یا سفارشی توسط یک شخص ثالث انجام می‌گیرد.

۶-٤: از فرآیندها و روش‌های کنترل تغییر برای تمام تغییرات اجزای سیستم تبعیت شود.

۶-۵: از آسیب‌پذیری‌های رمزگذاری رایج در فرآیندهای توسعه نرم‌افزار با آموزش توسعه‌دهندگان در تکنیک‌های برنامه‌نویسی امن و توسعه برنامه‌های کاربردی بر اساس دستورالعمل برنامه نویسی امن جلوگیری شود از جمله اینکه چگونه اطلاعات حساس در حافظه به‌کار رود.

۶-۶: تمام برنامه‌های کاربردی وب عمومی بایستی در برابر حملات شناخته شده محافظت شود؛ در مقابل برنامه‌های کاربردی وب عمومی، یا از طریق انجام ارزیابی آسیب‌پذیری نرم‌افزار حداقل سالانه و بعد از هر گونه تغییر و یا به وسیله نصب یک راهکار خودکار فنی که حملات مبتنی بر وب را تشخیص و از آن جلوگیری می‌کند (برای مثال، فایروال وب-نرم‌افزار)، به طور مستمر تمام ترافیک بررسی شود.

۶-۷: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

۴) هدف ۴- اعمال تمهیدات قوی در کنترل دسترسی‌ها:

کنترل دسترسی، مجوز استفاده یا عدم استفاده از وسایل فیزیکی یا فنی برای دسترسی به PAN و سایر اطلاعات دارنده کارت است. دسترسی باید بر اساس نیاز هر کسب و کار متفاوت باشد. کنترل دسترسی فیزیکی مستلزم استفاده از قفل و یا ابزار دیگری برای محدود کردن دسترسی به کامپیوتر، سوابق مبتنی بر کاغذ و یا سخت افزار سیستم می‌باشد. کنترل دسترسی منطقی اجازه یا رد استفاده از دستگاه‌های پرداخت، شبکه‌های بی‌سیم، رایانه‌های شخصی و دیگر دستگاه‌های محاسباتی و همچنین کنترل دسترسی به فایل‌های دیجیتال شامل اطلاعات دارنده کارت است.

الزام ۷- محدود کردن دسترسی به اطلاعات دارندگان کارت‌ها در حداقل احتیاج هر کسب و کار:

برای اطمینان از اینکه داده‌های حساس تنها در دسترس پرسنل مجاز باشد، سیستم‌ها و فرآیندها باید برای محدود کردن دسترسی براساس نیاز کسب و کار و با توجه به مسئولیت‌های شغلی باشد. حقوق دسترسی از حداقل مقدار داده‌ها و امتیازات مورد نیاز برای انجام یک شغل داده می‌شود.

فرآیندها و کنترل‌های امنیتی لازم:

۷-۱: دسترسی به اجزای سیستم و اطلاعات دارنده کارت فقط به آن دسته از افرادی که بر حسب شغلشان نیاز به چنین دسترسی دارند محدود شود.

۷-۲: یک سیستم کنترل دسترسی برای اجزای سیستم تاسیس شود که دسترسی بر اساس نیاز کاربر به دانستن را محدود کند، و همه را به جز افراد مجاز خاص انکار کند.

۷-۳: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

الزام ۸- شناسایی و احراز هویت دسترسی به اجزای سیستم:

اختصاص کد شناسایی منحصر به فرد (ID) به هر فرد دارای دسترسی، مجاز بودن آنان برای انجام و پیگیری اقدامات بر روی داده‌ها و سیستم‌های حساس را تضمین می‌کند. این الزامات بایستی روی تمام حساب‌ها اعمال می‌شود، از جمله حساب‌های پایانه‌های فروش، با قابلیت مدیریتی و تمام حساب‌های با دسترسی به ذخیره اطلاعات دارنده کارت.

فرآیندها و کنترل‌های امنیتی لازم:

۸-۱: سیاست‌ها و روش‌هایی برای اطمینان از مدیریت مناسب شناسایی کاربر برای کاربران و مدیران کل اجزاء سیستم تعریف و پیاده‌سازی گردد. یک نام کاربری منحصر به فرد برای تمام کاربران قبل از اجازه دسترسی به اجزای سیستم و یا اطلاعات دارنده کارت، اختصاص داده شود.

۸-۲: بکارگیری حداقل یکی از موارد ذیل برای احراز هویت تمام کاربران الزامی است:

- آنچه که شما می‌دانید، مانند یک کلمه یا عبارت عبور،
- آنچه که شما دارید، مانند دستگاه توکن یا کارت‌های هوشمند؛
- و یا آنچه که شما هستید، مانند بیومتریک، مشخصات فیزیکی یا رفتاری.

از روش‌های احراز هویت قوی استفاده نموده و تمام کلمات عبور در طول انتقال و ذخیره سازی با استفاده از رمزنگاری قوی ناخوانا شود.

۸-۳: احراز هویت دوعاملی برای کل دسترسی‌های از راه دور به شبکه از خارج از شبکه، توسط کارمندان، مدیران، و اشخاص ثالث از جمله دسترسی به فروشنده برای پشتیبانی و یا تعمیر و نگهداری، اجرا شود. نمونه ای از تکنولوژی دوعاملی، احراز هویت از راه دور و سرویس dial-in (RADIUS) با توکن؛ سیستم کنترل دسترسی کنترل‌کننده‌های دسترسی ترمینال‌ها (TACACS) با توکن و ... می‌باشد. استفاده دو مرتبه از یک عامل (به عنوان مثال با استفاده از دو کلمه عبور جداگانه) احراز هویت دوعاملی محسوب نمی‌شود.

۸-٤: سیاست‌ها و روش‌های احراز هویت برای تمام کاربران ایجاد، پیاده‌سازی، و ارسال گردد.

۸-٥: از ID های گروهی، اشتراکی، یا عمومی، و یا سایر روش‌های احراز هویت استفاده نشود. ارائه‌دهندگان خدمات با دسترسی به محیط‌های مشتری باید از یک اعتبارنامه احراز هویت منحصر به فرد (مانند یک کلمه یا عبارت عبور) برای هر محیط مشتری استفاده نمایند.

۸-٦: استفاده از سایر مکانیسم‌های احراز هویت مانند توکن امنیت فیزیکی، کارت‌های هوشمند، و گواهی باید به یک حساب شخصی اختصاص داده شود.

۸-۷: دسترسی‌ها به پایگاه داده حاوی اطلاعات دارنده کارت باید محدود شود: دسترسی همه کاربران باید از طریق روش‌های برنامه ریزی شده باشد؛ تنها مدیران پایگاه داده می‌توانند دسترسی مستقیم و یا Query داشته باشند؛ و ID نرم‌افزار برنامه‌های کاربردی

پایگاه داده تنها می‌تواند توسط برنامه‌های کاربردی استفاده شود (و نه کاربران و یا فرآیندهای غیر نرم‌افزاری).

۸-۸: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

الزام ۹- محدود کردن دسترسی فیزیکی به اطلاعات دارندگان کارت‌ها:

هر دسترسی فیزیکی به داده‌ها یا سیستم‌هایی که محل اطلاعات دارنده کارت است، فرصتی برای دسترسی و یا حذف دستگاه‌ها، اطلاعات، سیستم و یاهاردکپی‌ها برای افراد مهیا می‌کند؛ بنابراین بایستی به صورت مناسب محدود شود. کارکنان تمام وقت و پاره وقت، کارکنان موقت، پیمانکاران و مشاوران که از نظر فیزیکی در محل حاضر هستند، "پرسنل" نامیده می‌شوند. فروشندگان و مهمانان که برای مدت زمان کوتاه (معمولا تا یک روز) وارد مرکز می‌شوند "بازدیدکننده" هستند. تمام رسانه‌های کاغذی و الکترونیکی حاوی اطلاعات دارنده کارت"رسانه" می‌باشد.

فرآیندها و کنترل‌های امنیتی لازم:

۹-۱ : از کنترل مناسب ورود برای محدود کردن و نظارت بر دسترسی فیزیکی به سیستم در محیط اطلاعات دارنده کارت استفاده گردد.

۹-۲ : روشی برای تمایز آسان میان پرسنل و بازدید کنندگان، مانند اختصاص ID ایجاد شود.

۹-۳: دسترسی فیزیکی پرسنل به مناطق حساس کنترل شود. دسترسی باید مجاز و بر اساس عملکرد شغلی فرد باشد؛ دسترسی باید بلافاصله پس از ختم لغو شود، و تمام مکانیزم‌های دسترسی فیزیکی، مانند کلید، کارت‌های دسترسی، و غیره بازگشت و یا غیر فعال شود.

۹-٤: تمامی بازدید کنندگان قبل از ورود به مناطقی که در آن اطلاعات دارنده کارت پردازش و یا نگهداری می‌شود بایستی مجاز باشند؛ توکن‌های فیزیکی برای شناسایی

بازدیدکننده گان غیر از پرسنل که دارای تاریخ انقضا می‌باشد داده شود؛ و قبل از خروج از مرکز و یا در تاریخ انقضا پس گرفته شود. از log بازدیدکننده برای نگهداری audit trail فیزیکی اطلاعات و فعالیت‌های بازدیدکننده از جمله نام بازدید کننده، شرکت، و دسترسی فیزیکی مجاز پرسنل استفاده شود. Log مربوطه را حداقل سه ماه نگهداری شود مگر اینکه توسط قانون محدود شده باشد.

۹-۵: تمام رسانه‌ها از لحاظ فیزیکی امن گشته و پشتیبان‌های[1] رسانه در یک مکان امن ترجیحا خارج از سایت ذخیره شود.

۹-٦: کنترل دقیق بر روی توزیع داخلی و خارجی از هر نوع رسانه وجود داشته باشد.

۹-۷: کنترل دقیق بر روی ذخیره سازی و دسترسی به رسانه‌ها وجود داشته باشد.

۹-۸: رسانه‌ها در صورت عدم نیاز کسب و کار به آن یا دلایل قانونی نابود شود.

۹-۹: دستگاه‌هایی که اطلاعات کارت پرداخت از طریق تعامل فیزیکی مستقیم با کارت در آن ثبت می‌شود، در برابر tampering و تعویض محافظت گردد. این الزام از طریق بازرسی‌های دوره ای از سطوح دستگاه POS برای تشخیص tampering، و آموزش پرسنل جهت آگاهی از فعالیت‌های مشکوک انجام می‌گیرد.

۹-۱۰: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

۵) هدف ۵- پایش و ارزیابی مداوم شبکه:

شبکه‌های فیزیکی و بی‌سیم اتصال پیوسته با تمام نقاط پایانی و سرور در زیرساخت پرداخت دارند. آسیب‌پذیری در دستگاه‌ها و سیستم‌های شبکه فرصت دسترسی غیر مجاز به برنامه‌های کاربردی کارت پرداخت و اطلاعات دارنده کارت را برای مجرمان فراهم می‌آورد. برای جلوگیری از سوء استفاده، بایستی سازمان‌ها به طور مرتب شبکه را جهت یافتن و رفع آسیب‌پذیری‌ها نظارت و تست کنند.

[1] Backup

الزام ۱۰- پایش و ردیابی مداوم هرگونه دسترسی به منابع اطلاعاتی، تجهیزات شبکه و همچنین اطلاعات مربوط به دارندگان کارت‌ها:

مکانیزم ورود و توانایی ردیابی فعالیت کاربران برای مدیریت موثر آسیب‌پذیری و تشخیص جرم بسیار مهم است. حضور logها در تمامی محیط‌ها، ردیابی و آنالیز دقیق در صورت وجود اشتباه را ممکن می‌سازد. تعیین علت خطر بدون log فعالیت سیستم، بسیار دشوار است.

فرآیندها و کنترل‌های امنیتی لازم:

۱۰-۱: audit trailهایی برای ارتباط با تمام دسترسی‌های اجزای سیستم به هر کاربر داده شود.

۱۰-۲: audit trailهای خودکار برای تمامی اجزای سیستم جهت بازسازی وقایع به شرح ذیل پیاده‌سازی گردد:

- دسترسی هر کاربر فردی به اطلاعات دارندگان؛
- تعیین تمام اقدامات صورت گرفته توسط هر فرد با دسترسی مدیریتی یا ریشه ای؛
- دسترسی به تمام audit trailها؛
- تلاش‌های دسترسی منطقی نامعتبر؛
- استفاده و تغییر مکانیزم شناسایی و احراز هویت (از جمله ایجاد حساب جدید، ترفیع امتیازات)، و تمام تغییرات، اضافات و حذف حساب با دسترسی مدیریتی؛
- مقدار دهی اولیه، توقف یا مکث logهای audit؛
- ایجاد و حذف موضوعات در سطح سیستم.

۱۰-۳: مطالب audit trail برای تمام اجزای سیستم برای هر رویداد که حداقل شامل: شناسایی کاربر، نوع رویداد، تاریخ و زمان، نشانه موفقیت یا شکست، منشاء رویداد، و هویت و یا نام داده آسیب‌دیده، اجزا و یا منابع سیستم است، ثبت شود.

۱۰-٤: با استفاده از تکنولوژی سنکرون سازی زمان، ساعت سیستم‌های حیاتی را سنکرون نموده و زمان پذیرندگی، توزیع و ذخیره سازی کنترل شود.

۱۰-۵: audit trail امن شود به طوری که نتواند جایگزین گردد.

۱۰-٦: logها و رویدادهای امنیتی برای همه اجزای سیستم جهت شناسایی اشکالات و یا فعالیت‌های مشکوک بررسی شود. logهای مهم حداقل روزانه بررسی شود.

۱۰-۷: سابقه audit trail برای حداقل یک سال نگهداری شود؛ حداقل سابقه سه ماهه برای آنالیز آنی بایستی در دسترس باشد.

۱۰-۸: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

الزام ۱۱- ارزیابی منظم و قاعده‌مند امنیت سیستم‌ها و فرآیندهای امنیتی لحاظ شده:

آسیب‌پذیری‌ها توسط افراد و محققان مخرب کشف و توسط نرم‌افزارهای جدید ارائه می‌گردند. اجزای سیستم، فرایندها و نرم‌افزارهای سفارشی بایستی به طور مرتب جهت اطمینان از امنیت در کل طول زمان تست شود. تست کنترل‌های امنیتی برای هر گونه تغییر محیطی مانند استقرار نرم‌افزار جدید و یا تغییر تنظیمات سیستم مهم است.

جدول ۲-۳: میزان شدت اسکن آسیب‌پذیری

امتیاز CVSS[1]	میزان شدت	نتیجه اسکن
۷ از ۱۰	شدت بالا	ناموفق
٤ از ٦/۹	شدت متوسط	ناموفق
۰ از ۳/۹	شدت پایین	موفق

فرآیندها و کنترل‌های امنیتی لازم:

۱۱-۱: فرآیندهایی جهت تست حضور نقاط دسترسی بی‌سیم (802.11) و تشخیص و شناسایی تمامی نقاط دسترسی بی‌سیم مجاز و غیر مجاز در دوره‌های سه ماهه اجرا گردد.

[1] Common Vulnerability Scoring System

فهرستی از نقاط دسترسی بی‌سیم مجاز ایجاد و رویه پاسخ به رویدادها در صورت شناسایی نقاط دسترسی بی‌سیم غیر مجاز پیاده‌سازی گردد.

۱۱-۲: آسیب‌پذیری‌های شبکه داخلی و خارجی حداقل هر سه ماه و بعد از هر تغییر قابل توجهی در شبکه اسکن شود. در صورت نیاز تا زمان اجرای اسکن قابل پذیرش دوباره اسکن شود. پس از یک اسکن قابل پذیرش برای انطباق اولیه PCI DSS، یک نهاد بایستی در سال‌های پس از آن، چهار اسکن متوالی سه ماهه را به عنوان یک الزام برای انطباق اجرا کند. اسکن خارجی سه ماهه باید توسط یک Approved Scanning Vendor (ASV) انجام شود. هر اسکن پس از تغییرات در شبکه و اسکن داخلی توسط کارکنان داخلی انجام می‌گردد.

۱۱-۳: یک روش برای تست نفوذ (تست نفوذ خارجی و داخلی) حداقل در دوره‌های سالیانه و بعد از هر گونه ارتقاء و یا اصلاح ایجاد و پیاده‌سازی شود.

۱۱-٤: از تکنیک‌های تشخیص نفوذ به شبکه و / یا جلوگیری از نفوذ برای شناسایی و / یا جلوگیری از نفوذ به شبکه استفاده شود. کل ترافیک محیط پیرامون اطلاعات دارنده کارت و همچنین نقاط بحرانی در داخل محیط اطلاعات دارنده کارت مانیتور شده و در موارد مشکوک به پرسنل هشدار داده شود. موتورهای IDS / IPS (Intrusion Detection System / Intrusion Prevention System)، خطوط مبنا، و امضاها بایستی به روز نگه داشته شود.

۱۱-۵: یک مکانیزم تشخیص تغییر (به عنوان مثال، ابزار یکپارچه نظارتی) جهت هشدار به پرسنل در مواقع تغییرات غیر مجاز فایل‌های بحرانی سیستم، فایل‌های پیکربندی و یا فایل‌های محتوایی (از جمله تغییرات، اضافات، و حذف) استقرار گردد. نرم‌افزار برای انجام مقایسه فایل‌های مهم حداقل هفته ای یکبار تنظیم شود. یک فرایند برای پاسخ به هر گونه هشدار تولید شده توسط راهکار تشخیص تغییر پیاده‌سازی شود.

۱۱-٦: سیاست‌های امنیتی و روش‌های عملیاتی مستند شده، مورد استفاده قرار گرفته و برای طرفین درگیر شناخته شده باشد.

۶) هدف ۶- اتخاذ یک سیاست امنیت اطلاعات:

یک سیاست امنیتی قوی وظایف مربوط به امنیت کارکنان یک سازمان را تعیین می‌نماید. همه کارکنان باید از حساسیت اطلاعات دارنده کارت و مسئولیت‌های خود برای حفاظت از آن آگاه باشند.

الزام ۱۲- سیاستی اتخاذ شود که خط مشی‌های امنیت اطلاعات در آن برای تمام پرسنل مشخص گردد:

یک سیاست امنیتی قوی برای کل سازمان تدوین شده و وظایف پرسنل به اطلاعشان برسد. همه پرسنل باید از حساسیت اطلاعات دارنده کارت و مسئولیت‌های خود برای حفاظت از آن آگاه باشند.

فرآیندها و کنترل‌های امنیتی لازم:

۱۲-۱: یک سیاست امنیتی تاسیس، انتشار، نگهداری شود و حداقل در دوره‌های یک ساله با توجه به تغییرات محیطی بررسی و به روز رسانی گردد.

۱۲-۲: یک فرایند رسمی ارزیابی خطر پیاده‌سازی گردد و حداقل در دوره‌های یک ساله و به محض ایجاد تغییرات قابل توجه در محیط از جمله دارایی‌ها، تهدید، و آسیب‌پذیری‌های مهم اجرا گردد.

۱۲-۳: سیاست‌های کاربردی برای فن آوری‌های مهم جهت استفاده مناسب از آن توسط پرسنل ایجاد شود. این خدمات عبارتند از دسترسی از راه دور، بی‌سیم، رسانه‌های الکترونیکی قابل حمل، لپ تاپ، تبلت، دستگاه‌های دستی، ایمیل و اینترنت.

۱۲-۴: سیاست و روش‌های امنیتی بایستی به وضوح مسئولیت امنیت اطلاعات برای تمام پرسنل را تعیین نماید.

۱۲-۵: مسئولیت‌های گروهی و یا فردی جهت امنیت اطلاعات به پرسنل اختصاص گردد.

۱۲-۶: برنامه رسمی شناخت امنیت برای آگاهی پرسنل از اهمیت امنیت اطلاعات دارنده کارت اجرا شود.

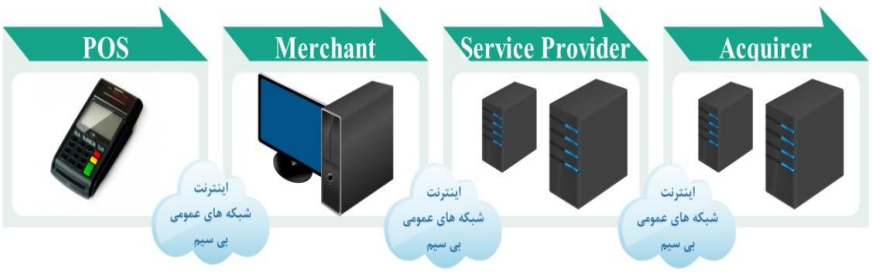
۱۲-۷: جهت به حداقل رساندن خطر حملات منابع داخلی، پرسنل بالقوه قبل از استخدام از لحاظ سابقه اشتغال، سابقه کیفری، سابقه اعتبار و چک‌های برگشتی بررسی گردند.

۱۲-۸: سیاست‌ها و روش‌هایی برای مدیریت ارائه‌دهندگان خدمات جهت تعیین اینکه چه اطلاعاتی از دارنده کارت می‌تواند به اشتراک گذاشته و یا می‌تواند بر امنیت اطلاعات دارنده کارت تاثیر بگذارد، برقرار و اجرا شود.

۱۲-۹: الزام اضافی تنها برای ارائه‌دهندگان خدمات: ارائه‌دهندگان خدمات بایستی به مشتریان اقرار کنند که آنها مسئول امنیت اطلاعات دارنده کارتی هستند که به نمایندگی از مشتریان صدور و یا ذخیره، پردازش، و انتقال آن را به عهده دارند و یا تا حدی آنها می‌توانند بر امنیت محیط اطلاعات دارنده کارت تاثیر بگذارند.

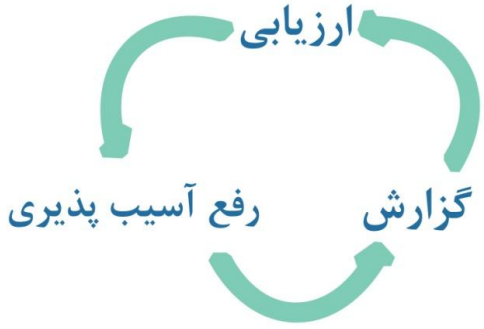
۱۲-۱۰: یک طرح پاسخ رویداد اجرا شود. آمادگی برای پاسخ فوری به نقض سیستم وجود داشته باشد.

مراحل صحت‌سنجی تطبیق با استاندارد PCI DSS



شکل ۲-۳: اجزای شبکه

جهت پیوستن به PCI DSS بایستی ۳ گام به شرح ذیل که فرآیندی مداوم است انجام گیرد:



شکل ۲-۴: مراحل انطباق

۱) **ارزیابی (Assess) :**

در این مرحله تمام مکان‌های اطلاعات دارنده کارت شناسایی و فهرستی از دارایی‌های IT و فرآیند کسب وکار مرتبط با پردازش کارت پرداخت تهیه شده و از نظر آسیب‌پذیری‌هایی که ممکن است اطلاعات دارنده کارت را تحت الشعاع قرار دهد، بررسی می‌گردد.

هدف اولیه این ارزیابی، شناخت آسیب‌پذیری‌های تکنولوژی و فرآیندها است که ممکن است امنیت اطلاعات صاحب کارت را هنگام انتقال، پردازش یا ذخیره سازی، در معرض خطر قرار دهد.

۲) **رفع آسیب‌پذیری‌ها (Repair) :**

در این مرحله آسیب‌پذیری‌های شناخته شده رفع شده، اطلاعات غیرضروری ذخیره شده دارنده کارت به صورت امن حذف و فرآیندهای کسب و کار امن پیاده‌سازی می‌گردد.

۳) **گزارش (Report)**

تمام دارایی‌ها و جزئیات بازسازی‌ها مستند شده، و گزارش انطباق به بانک پذیرنده و برند کارت یا هر نهادی که تجارت با آنها انجام می‌گیرد، ارسال شود.

آنچه به منظور صحت سنجی انطباق بایستی انجام گیرد به شرح ذیل است:

۱) انتخاب ارزیاب امنیت ماهر (QSA[1])

ارزیاب امنیت ماهر (QSA) یک شرکت امنیتی داده‌ها است که توسط شورای استانداردهای امنیتی PCI واجد شرایط به انجام ارزیابی PCI DSS در محل می‌باشد. QSA بایستی فرآیندهای ذیل را اجرا نماید:

- بررسی تمام اطلاعات فنی داده شده توسط پذیرنده و یا ارائه‌دهنده خدمات
- استفاده از قضاوت مستقل به منظور تایید استاندارد
- ارائه پشتیبانی و راهنمایی در طول فرایند انطباق
- حضور در محل در طول مدت زمان ارزیابی مورد نیاز
- پایبند به روش‌های ارزیابی امنیت PCI DSS
- اعتبارسنجی دامنه ارزیابی
- ارزیابی جبران کنترل
- تهیه گزارش نهایی

۲) انتخاب یک Approved Scanning Vendor (ASV)

ASV یک شرکت امنیت داده‌ها است که با استفاده از یک راهکار اسکن، موارد آسیب‌پذیری‌های خارجی را تعیین می‌نماید. ASVها توسط شورای استانداردهای امنیتی PCI واجد شرایط جهت انجام اسکن خارجی شبکه و سیستم مورد نیاز PCI DSS می‌باشند. ASV ممکن است نرم‌افزار خود و یا یک راهکار تجاری open source تاییدشده را استفاده کند.

۳) دامنه الزامات PCI DSS:

[1] Qualified Security Assessor

اولین مرحله PCI DSS تعیین دقیق محدوده محیط است. فرایند شناسایی دامنه شامل تمامی اجزای سیستم است که در داخل آن قرار دارد و یا به آن متصل است. محیط اطلاعات دارنده کارت متشکل از مردم، فرآیندها و فناوری کنترل داده‌های دارنده کارت یا داده‌های حساس احراز هویت می‌باشد. اجزای سیستم شامل دستگاه‌های شبکه (هر دو سیمی و بی‌سیم)، سرورها و برنامه‌های کاربردی، اجزای مجازی سازی مانند ماشین‌های مجازی، سوئیچ / روترهای مجازی ، لوازم مجازی، برنامه / دسکتاپ‌های مجازی ، و hypervisorها است.

هدف گذاری باید حداقل سالانه و قبل از ارزیابی سالانه انجام شود. نهادها باید همه مکان‌ها و جریان اطلاعات دارنده کارت، تمام سیستم‌های متصل و تاثیرگذار بر محیط اطلاعات دارنده کارت CDE[1] (مانند سرور احراز هویت) را شناسایی نمایند.

سازمان‌ها جهت تایید دقت و صحت CDE تعریف شده مراحل زیر را بایستی انجام دهند:

- نهاد ارزیابی بایستی وجود تمام اطلاعات دارنده کارت در محیط را به منظور بررسی اینکه هیچ اطلاعات دارنده کارت در خارج از CDE وجود ندارد، شناسائی و ثبت کند.
- زمانی که تمامی محل‌های اطلاعات دارنده کارت شناسایی و مستند شد، نهاد مربوطه از نتایج به منظور بررسی مناسب دامنه PCI DSS استفاده نماید. (برای مثال، نتایج ممکن است یک نمودار یا فهرستی از مکان‌های اطلاعات دارنده کارت باشد).
- اطلاعات دارنده کارت بایستی در حوزه ارزیابی PCI DSS و بخشی از CDE باشد. اگر مشخص شود که داده شامل CDE نمی‌شود، باید به صورت امن حذف شود.
- اسناد دامنه PCI DSS برای ارزیابی و / یا برای مرجع تعیین دامنه بعدی سالانه PCI DSS حفظ شود.

۴) استفاده از پرسشنامه خود ارزیابی (SAQ[1])

[1] Cardholder Data Environment

"SAQ" یک ابزار اعتبار سنجی برای ارائه‌دهندگان خدمات جهت گزارش نتایج خودارزیابی PCI DSS در صورت الزامی نبودن ROC[2] است. SAQ شامل مجموعه ای از سوالات بله یا خیر برای هر کدام از الزامات PCI DSS است. در صورت پاسخ منفی سازمان بایستی تاریخ اصلاح آتی را اعلام و اقدامات مرتبط را انجام دهد.

۵) گزارش انطباق (ROC):

گزارش یک مکانیسم رسمی جهت گزارش وضعیت انطباق با PCI DSS است. بسته به الزامات برند کارت پرداخت، ارائه‌دهندگان خدمات ممکن است نیاز به یک SAQ برای خود ارزیابی، و یا یک گزارش تطبیق برای ارزیابی داشته باشند. ارسال گزارش سه ماهه برای اسکن شبکه نیز ممکن است مورد نیاز باشد.

اطلاعات موجود در گزارش تطبیق:

- خلاصه اجرایی (شرح کسب و کار کارت پرداخت؛ نمودار شبکه در سطح بالا)
- شرح محدوده کار و رویکرد (شرح چگونگی ارزیابی، محیط، قطعه بندی شبکه، و جزئیات هر مجموعه نمونه انتخاب و تست شده، سازمان‌های کاملا متعلق و یا بین المللی نیازمند به انطباق با PCI DSS، شبکه‌های بی‌سیم و یا برنامه‌های کاربردی که می‌تواند امنیت اطلاعات دارنده کارت را تحت تاثیر قرار دهد، نسخه PCI DSS مورد استفاده برای انجام ارزیابی)
- جزئیات مورد بررسی محیط (نمودار هر شبکه، شرح محیط اطلاعات دارنده کارت، لیستی از تمام سخت افزار و نرم‌افزار موجود در CDE، ارائه‌دهندگان خدماتی که استفاده شده، برنامه‌های کاربردی پرداخت شخص سوم، افرادی که مصاحبه شده‌اند، اسناد مرور شده، جزئیات بررسی ارائه‌دهندگان خدمات مدیریت شده)
- اطلاعات تماس و تاریخ گزارش

---

[1] Self-Assessment Questionnaire
[2] Report on Compliance

- نتایج سه ماهه اسکن (خلاصه ای از نتایج چهار اسکن اخیر ASV)
- یافته‌ها و مشاهدات (یافته‌های دقیق در مورد هر الزام اصلی و فرعی، از جمله توضیح پاسخ‌های N/A و اعتبار کنترل خسارت)

۶) پیاده‌سازی PCI DSS در فرآیندهای معمول کسب و کار:

برای اطمینان از درستی پیاده‌سازی کنترل‌های امنیتی، PCI DSS بایستی در فرآیندهای معمول کسب و کار (BAU[1]) به عنوان بخشی از استراتژی کلی امنیت یک نهاد اجرا گردد، تا اثربخشی آن به صورت مداوم نظارت شده و محیط منطبق بر PCI DSS در فاصله هر ارزیابی حفظ شود. نمونه‌هایی از best practiceها برای ترکیب PCI DSS با BAU شامل (اما نه محدود به) موارد به شرح ذیل است:

- کنترل‌های امنیتی به منظور اطمینان از عملکرد موثر آنها بر اساس آنچه در نظر گرفته شده بود نظارت شود.
- تضمین شود که همه شکست‌ها در کنترل‌های امنیتی شناسایی و به موقع پاسخ داده شود.
- تغییرات محیط (به عنوان مثال، افزودن سیستم‌های جدید، تغییر در سیستم و یا تنظیمات شبکه) قبل از دامنه PCI DSS بررسی شود.
- تغییر ساختار سازمان (به عنوان مثال، ادغام یا مالکیت شرکت‌ها) در نتیجه بررسی رسمی از تاثیر دامنه و الزامات PCI DSS.
- انجام بررسی‌ها و ارتباطات دوره ای به منظور تایید این که الزامات PCI DSS ادامه داشته و پرسنل فرآیندهای امن را دنبال کنند.
- بررسی فن‌آوری‌های سخت افزار و نرم‌افزار حداقل سالانه به منظور تایید این که آنها همچنان توسط فروشنده پشتیبانی شده و می‌توانند به الزامات امنیتی، از جمله PCI DSS پیوسته و با نواقص به شکل مناسب برخورد کنند.

[1] Business-As-Usual

فصل ۳

استاندارد امنیت داده‌های برنامه‌های کاربردی پرداخت PCI PA-DSS
(Payment Application - Data Security Standard)

مقدمه

PA-DSS مخفف Payment Application – Data Security Standard و استاندارد امنیت داده‌های برنامه‌های کاربردی پرداخت بوده و در راستای حفظ امنیت داده‌ها در نرم‌افزارهای کاربردی لازم است که این برنامه‌ها عملیات ذخیره‌سازی و پردازش و انتقال دو گونه داده شامل داده‌های دارنده کارت (مانند نام دارنده کارت و PAN) و داده‌های احراز هویت (مانند اطلاعات شیار ۲ و CVV2) کارت پرداخت را با پشتیبانی از استاندارد PA_DSS انجام دهند.

رعایت این استاندارد در محدوده زیر تعریف می‌شود:

- توابع و اجزاء پرداخت (End-to-End)
- ورودی و خروجی
- شرایط خطا
- رابط‌های کاربر و ارتباط با سایر سیستم‌ها، فایل‌ها، برنامه‌های پرداختی
- جریان داده‌های دارنده کارت
- مکانیزم‌های رمزنگاری
- مکانیزم‌های احراز هویت

اطلاعات کاربردی از PCI DSS:

PCI DSS توسط همه نهادهای درگیر در پردازش کارت پرداخت از جمله پذیرندگان، پردازنده‌ها، بانک‌های پذیرنده، صادرکنندگان، و ارائه دهندگان خدمات و سایر نهادهای درگیر در ذخیره، پردازش، و یا انتقال اطلاعات دارنده کارت و / یا داده‌های حساس احراز هویت کاربرد دارد.

اطلاعات دارنده کارت و اطلاعات حساس احراز هویت به صورت زیر تعریف می‌شود:

جدول ۳-۱: اطلاعات حساب

اطلاعات حساب	
اطلاعات دارنده کارت	اطلاعات حساس احراز هویت
➢ Primary Account Number (PAN) ➢ نام دارنده کارت ➢ تاریخ انقضا ➢ کد سرویس	➢ اطلاعات کامل مسیر (اطلاعات نوار مغناطیسی یا معادل آن بر روی یک تراشه) ➢ CAV2 / CVC2 / CVV2 / CID ➢ PIN / PIN Block

جدول ۳-۲: چگونگی ذخیره اطلاعات حساب

		نوع اطلاعات	مجوز ذخیره	ذخیره اطلاعات به صورت ناخوانا طبق الزام PA-DSS ۳-۲
اطلاعات حساب	اطلاعات دارنده کارت	Primary Account Number (PAN)	دارد	دارد
		نام دارنده کارت	دارد	ندارد
		Service Code	دارد	ندارد
		تاریخ انقضا	دارد	ندارد
	اطلاعات حساس احراز هویت	اطلاعات کامل مسیر	ندارد	طبق الزام ۱-۱ PA-DSS نمی‌تواند ذخیره شود
		CAV2 / CVC2 / CVV2 / CID	ندارد	طبق الزام ۱-۱ PA-DSS نمی‌تواند ذخیره شود
		PIN / PIN Block	ندارد	طبق الزام ۱-۱ PA-DSS نمی‌تواند ذخیره شود

الزامات استاندارد PA-DSS

این استاندارد ۱۴ الزام برنامه‌های کاربردی پرداخت برای هر کسب و کاری، اعم از فروشندگان نرم‌افزار، شرکت‌های ارایه دهنده خدمات پرداخت، بانک‌ها و مشتریان در نظر گرفته است که این الزامات، یک چارچوب کاری برای محیط امن برنامه کاربردی پرداخت را تعریف می‌کند. این الزامات، عبارتند از:

جدول ۳-۳: الزامات استاندارد PA-DSS

الزامات PA-DSS
الزام ۱: اطلاعات کامل، از جمله کد یا مقدار امنیتی کارت (CAV2[1]، CID[2]، CVC2[3]، CVV2[4])، و یا اطلاعات PIN block نگهداری نشود.
الزام ۲: از اطلاعات ذخیره شده دارنده کارت محافظت گردد.
الزام ۳: ویژگی‌های احراز هویت امن ارائه شود.
الزام ۴: فعالیت‌های برنامه کاربردی پرداخت ثبت گردد.
الزام ۵: برنامه‌های کاربردی پرداخت امن ایجاد شود.
الزام ۶: از انتقال بی سیم محافظت شود.
الزام ۷: برنامه‌های کاربردی پرداخت جهت شناسایی آسیب پذیری‌ها تست و آپدیت شود.
الزام ۸: پیاده سازی شبکه امن تسهیل شود.
الزام ۹: اطلاعات دارنده کارت نباید هرگز در سرور متصل به اینترنت ذخیره شود.
الزام ۱۰: دسترسی امن از راه دور به برنامه کاربردی پرداخت تسهیل شود.
الزام ۱۱: ترافیک حساس بر روی شبکه‌های عمومی رمزگذاری گردد.
الزام ۱۲: تمام دسترسی‌های مدیریتی غیرکنسول ر رمزگذاری شود.
الزام ۱۳: الزامات پیاده سازی PA-DSS برای مشتریان، فروشندگان و یکپارچه سازان ارائه شود.
الزام ۱۴: مسئولیت‌های PA-DSS برای پرسنل اختصاص یافته، و برنامه‌های آموزشی برای پرسنل، مشتریان، نمایندگان فروش و یکپارچه سازان ارائه گردد.

۱) الزام ۱

اطلاعات کامل، از جمله کد یا مقدار امنیتی کارت (CAV2، CID، CVC2، CVV2)، و یا اطلاعات PIN block نگهداری نشود.

[1] Card Authentication Value
[2] Card Identification Number
[3] Card Verification Code
[4] Card Verification Value

الزام ۱-۱:

اطلاعات حساس احراز هویت بعد از عمل احراز هویت (حتی اگر رمزگذاری شده باشد) ذخیره نشود. تمام اطلاعات حساس احراز هویت پس از اتمام فرآیند مجوزدهی، غیرقابل بازیابی گردد.

معادل با الزام ۳-۲ PCI DSS

اطلاعات حساس احراز هویت در موارد ۱-۱-۱ الی ۱-۱-۳ شرح داده شده است.

الزام ۱-۱-۱: پس از مجوزدهی، محتویات کامل هر track نوار مغناطیسی (واقع در پشت یک کارت، اطلاعات معادل بر روی یک تراشه، و یا سایر مکان‌ها) ذخیره نشود. این اطلاعات به ترتیب track کامل، track، track 1، track 2، و اطلاعات نوار مغناطیسی نامیده می‌شود.

معادل با الزام ۳-۲-۱ PCI DSS

نکته: در یک جریان عادی کسب و کار، عناصر اطلاعات زیر از نوار مغناطیسی ممکن است نیاز به نگهداری داشته باشد:

- اسم دارنده کارت
- شماره حساب اصلی (PAN[1])
- تاریخ انقضا
- کد سرویس

برای به حداقل رساندن ریسک، تنها آن دسته از عناصر اطلاعات مورد نیاز کسب و کار ذخیره شود.

الزام ۱-۱-۲: پس از مجوزدهی، مقدار یا کد تأیید کارت (عدد سه یا چهار رقمی چاپ شده در جلو یا عقب کارت پرداخت که به منظور تأیید تراکنش‌های بدون حضور کارت استفاده می‌شود) ذخیره نشود.

[1] Primary Account Number

معادل با الزام ۳-۲-۲ PCI DSS

الزام ۱-۱-۳: پس از مجوزدهی، شماره شناسایی شخصی (PIN[1]) و یا PIN block رمز شده ذخیره نشود.

معادل با الزام ۳-۲-۳ PCI DSS

الزام ۱-۱-۴: هر گونه اطلاعات track (نوار مغناطیسی و یا اطلاعات معادل بر روی تراشه)، مقدار یا کد تأیید کارت، و تمام PINها و یا اطلاعات PIN block ذخیره شده توسط نسخه‌های قبلی برنامه کاربردی پرداخت به صورت امن (مطابق با استانداردهای پذیرفته شده صنعت) حذف شود، به عنوان مثال توسط لیستی از محصولات مورد تایید آژانس امنیت ملی، و یا سایر استانداردها یا مقررات ایالتی یا ملی.

معادل با الزام ۳-۲ PCI DSS

نکته: این الزام فقط در صورت ذخیره اطلاعات حساس احراز هویت توسط نسخه‌های قبلی برنامه کاربردی پرداخت به کار می‌رود.

الزام ۱-۱-۵: اطلاعات حساس احراز هویت بر روی سیستم‌های وندورها ذخیره نشود. اگر هرگونه اطلاعات حساس احراز هویت (اطلاعات قبل از مجوزدهی) بایستی برای اهداف اشکال‌یابی یا عیب یابی استفاده شود، از موارد ذیل اطمینان حاصل شود:

- اطلاعات حساس احراز هویت تنها در زمان نیاز برای حل یک مشکل خاص جمع‌آوری شود.
- این اطلاعات در یک محل خاص و شناخته شده با دسترسی محدود ذخیره شود.
- حداقل مقدار اطلاعات موردنیاز جهت رفع یک مشکل خاص جمع آوری شود.
- اطلاعات حساس احراز هویت با رمزنگاری قوی ذخیره شود.

[1] Personal Identification Number

- اطلاعات بلافاصله پس از استفاده به صورت امن از محل‌های ذیل حذف شود:
  - فایل log
  - فایل‌های اشکال زدایی
  - دیگر منابع اطلاعات دریافت شده از مشتریان.

معادل با الزام ۳-۲ PCI DSS

۲) الزام ۲:

از اطلاعات ذخیره شده دارنده کارت محافظت شود.

الزام ۲-۱:

فروشنده نرم‌افزار بایستی یک راهنما برای مشتریان در خصوص حذف امن اطلاعات دارنده کارت پس از انقضای دوره نگهداری تعریف شده مشتری فراهم نماید.

معادل با الزام ۳-۱ PCI DSS

الزام ۲-۲:

PAN به صورت پنهانی نمایش پنهان داده شود (حداکثر شش رقم اول و چهار رقم آخر نمایش داده شود)، به طوری که فقط افراد با نیاز کسب و کار مشروع بتوانند PAN کامل را ببینند.

معادل با الزام ۳-۳ PCI DSS

الزام ۲-۳:

PAN با استفاده از یکی از روش‌های زیر به صورت ناخوانا ذخیره شود (از جمله اطلاعات در رسانه‌های دیجیتال قابل حمل، رسانه‌های پشتیبان، و logها):

- هش یک طرفه بر اساس رمزنگاری قوی (هش باید از کل PAN باشد)
- کوتاه سازی (هش نمی‌تواند به عنوان جایگزین بخش کوتاه شده PAN استفاده شود)

- توکن‌ها و پدهای شاخص (پد باید به صورت امن ذخیره شود)
- رمزنگاری قوی همراه با فرآیندها و روش‌های مدیریت کلید.

معادل با الزام ۳-۴ PCI DSS

نکته ۱: بازسازی PAN اصلی از روی هر دو نسخه ناقص و درهم برای یک هکر نسبتا ساده است. زمانی که هر دو نسخه درهم و کوتاه شده PAN توسط برنامه کاربردی پرداخت تولید می‌شود، کنترل‌های اضافی بایستی جهت اطمینان از عدم توانایی بازسازی PAN انجام گیرد.

نکته ۲: PAN بایستی به صورت ناخوانا ذخیره شود، حتی در خارج از برنامه کاربردی پرداخت (به عنوان مثال، فایل log خروجی برنامه کاربردی برای ذخیره در محیط مشتری).

الزام ۲-۴:

برنامه کاربردی پرداخت بایستی از کلیدهای مورد استفاده برای تامین امنیت اطلاعات دارنده کارت در برابر افشا و سوء استفاده محافظت کند.

معادل با الزام ۳-۵ PCI DSS

نکته: این الزام برای کلید مورد استفاده در رمزگذاری اطلاعات ذخیره شده دارنده کارت، همچنین کلیدهای رمزنگاری کلید برای محافظت از کلیدهای رمزنگاری اطلاعات به کار می‌رود. کلیدهای رمزنگاری کلید باید حداقل به اندازه کلید رمزنگاری اطلاعات قوی باشد.

الزام ۲-۵:

برنامه کاربردی پرداخت بایستی فرآیندها و روش‌های مدیریت کلید را برای کلیدهای رمزنگاری اطلاعات دارنده کارت که شامل حداقل موارد ۲-۵-۱ الی ۲-۵-۷ باشد، پیاده‌سازی نماید.

معادل با الزام ۳-۶ PCI DSS

الزام ۲-۵-۱: تولید کلید رمزنگاری قوی

الزام ۲-۵-۲: توزیع امن کلید رمزنگاری

الزام ۲-۵-۳: ذخیره امن کلید رمزنگاری

الزام ۲-۵-۴: تغییرات کلید رمزنگاری برای کلیدهایی که به پایان دوره خود رسیده باشند (برای مثال، پس از یک دوره زمانی مشخص و / یا بعد از یک مقدار مشخصی از متن رمزنگاری شده که توسط یک کلید تولید شده است)، که این مقادیر توسط فروشنده نرم‌افزار و یا صاحب کلید، و بر اساس دستورالعمل صنعت (برای مثال، انتشارات ویژه NIST 800-57) تعریف می‌شود.

الزام ۲-۵-۵: کنار گذاشتن و یا جایگزینی کلید (برای مثال: با آرشیو، تخریب، و / یا ابطال) در صورت لزوم زمانی که یکپارچگی کلید تضعیف شده (برای مثال، خروج یک کارمند آگاه به کلید، و غیره) و یا کلید مشکوک به خطر می‌باشد.

نکته: اگر این کلیدها نیاز به نگهداری داشته باشد، بایستی به صورت امن بایگانی شود (برای مثال، با استفاده از یک کلید رمزنگاری کلید). کلیدهای رمزنگاری آرشیو باید تنها برای مقاصد رمزگشایی / تایید استفاده شوند.

الزام ۲-۵-۶: اگر برنامه کاربردی پرداخت از عملیات مدیریت کلید رمزنگاری دستی استفاده کند ، بایستی دانش تقسیم و کنترل دوگانه اجرا شود.

نکته: نمونه‌هایی از عملیات مدیریت کلید: تولید کلید، انتقال، بارگذاری، ذخیره سازی و تخریب است.

الزام ۲-۵-۷: پیشگیری از تعویض غیر مجاز کلیدهای رمزنگاری

الزام ۲-۶:

مکانیزمی برای عدم بازیابی مواد کلید رمزنگاری یا رمز ذخیره شده توسط برنامه کاربردی پرداخت، مطابق با استانداردهای پذیرفته شده صنعت فراهم شود.

این کلیدهای رمزنگاری برای رمزگذاری و یا تایید اطلاعات دارنده کارت استفاده می‌شود.

معادل با الزام ۳-۶ PCI DSS

۳) الزام ۳:

ویژگی‌های احراز هویت امن ارائه شود.

الزام ۳-۱:

برنامه کاربردی پرداخت بایستی از شناسه کاربری منحصر به فرد و احراز هویت امن برای دسترسی‌های مدیریتی و دسترسی به اطلاعات دارنده کارت استفاده نماید. احراز هویت امن باید در تمام حساب‌های تولید و یا مدیریت شده توسط برنامه کاربردی در مرحله تکمیل نصب و تغییرات بعدی پس از نصب اجرا شود.

معادل با الزام ۸-۱ و ۸-۲ PCI DSS

نکته: اصطلاح "تغییرات بعدی" اشاره دارد به تغییراتی که منجر به بازگشت به تنظیمات پیش فرض، ایجاد حساب جدید و یا ایجاد دوباره حساب‌های موجود می‌شود.

الزام ۳-۱-۱: برنامه کاربردی پرداخت از حساب‌های مدیریتی پیش فرض سایر نرم‌افزارهای موردنیاز استفاده نمی‌کند (برای مثال، برنامه کاربردی پرداخت نباید از حساب مدیریتی پیش فرض پایگاه داده استفاده کند).

معادل با الزام ۲-۱ PCI DSS

الزام ۳-۱-۲: برنامه کاربردی باید تمام کلمات عبور پیش فرض برنامه را برای همه حساب‌های تولید و یا مدیریت شده توسط برنامه در مرحله تکمیل نصب و تغییرات بعدی پس از نصب تغییر دهد.

این امر شامل همه حساب‌ها، از جمله حساب‌های کاربری، حساب برنامه کاربردی و سرویس، و حساب‌های مورد استفاده توسط فروشنده برای مقاصد پشتیبانی می‌باشد.

معادل با الزام ۲-۱ PCI DSS

نکته: این الزام نمی‌تواند از طریق تعیین یک فرایند کاربر و یا از طریق دستورالعمل راهنمای پیاده‌سازی PA-DSS برآورده شود. در پایان نصب و در زمان تغییرات بعدی، برنامه کاربردی باید از نظر فنی از رمز عبور پیش فرض جلوگیری نماید.

الزام ۳-۱-۳: برنامه کاربردی پرداخت شناسه منحصر به فرد برای حساب‌های کاربر اختصاص دهد.

معادل با الزام PCI DSS ۸-۱-۱

الزام ۳-۱-۴: برنامه کاربردی پرداخت بایستی حداقل یکی از روش‌های زیر را جهت احراز هویت کاربران به کار برد:

- آنچه که شما می‌دانید، مانند یک کلمه یا عبارت عبور،
- آنچه که شما دارید، مانند دستگاه توکن یا کارت‌های هوشمند؛
- و یا آنچه که شما هستید، مانند بیومتریک، مشخصات فیزیکی یا رفتاری.

معادل با الزام PCI DSS ۸-۲

الزام ۳-۱-۵: برنامه کاربردی پرداخت از حساب‌ها و یا کلمات عبور گروهی، اشتراکی و یا عمومی استفاده ننماید.

معادل با الزام PCI DSS ۸-۵

الزام ۳-۱-۶: کلمه عبور برنامه کاربردی پرداخت باید دارای الزامات ذیل باشد:

- حداقل طول هفت کاراکتر.
- شامل کاراکترهای عددی و حروفی.

الزام ۳-۱-۷: برنامه کاربردی پرداخت نیاز به تغییر کلمه عبور کاربر حداقل هر ۹۰ روز یکبار داشته باشد.

معادل با الزام PCI DSS ۸-۲-۴

الزام ۳-۱-۸: برنامه کاربردی پرداخت سابقه رمز عبور را نگه داشته و رمز عبوری متفاوت با چهار کلمه عبور اخیر را بپذیرد.

معادل با الزام PCI DSS ۵-۲-۸

الزام ۳-۱-۹: پس از شش مرتبه ورود ناموفق حساب کاربری را قفل کند.

معادل با الزام PCI DSS ۶-۱-۸

الزام ۳-۱-۱۰: مدت زمان قفل حساب کاربری به حداقل ۳۰ دقیقه تنظیم شود.

معادل با الزام PCI DSS ۷-۱-۸

الزام ۳-۱-۱۱: اگر یک جلسه در برنامه کاربردی پرداخت بیش از ۱۵ دقیقه غیر فعال باشد، جهت فعالسازی نیاز به احراز هویت دوباره داشته باشد.

معادل با الزام PCI DSS ۸-۱-۸

الزام ۳-۲:

فروشنده نرم‌افزار باید برای مشتریانی که با برنامه کاربردی پرداخت به PC، سرور، پایگاه داده با یک ID کاربر منحصر به فرد و احراز هویت امن دسترسی دارند یک راهنما فراهم نماید.

معادل با الزام PCI DSS ۱-۸ و ۲-۸

الزام ۳-۳:

تمام کلمات عبور برنامه کاربردی پرداخت در زمان انتقال و ذخیره سازی ایمن گردد (از جمله کلمه عبور برای کاربر و حساب).

معادل با الزام PCI DSS ۱-۲-۸

الزام ۳-۳-۱: استفاده از رمزنگاری قوی برای ناخوانا نمودن تمام کلمات عبور در زمان انتقال.

الزام ۳-۳-۲: استفاده از الگوریتم رمزنگاری قوی، یک طرفه، بر اساس استانداردهای تایید شده برای ناخوانا نمودن تمام کلمات عبور در زمان ذخیره سازی.

هر رمز عبور باید یک متغیر ورودی منحصر به فرد داشته باشد که به رمز عبور قبل از بکارگیری الگوریتم رمزنگاری پیوست شود.

نکته: این متغیر ورودی الزامی جهت غیرقابل پیش بینی و یا مخفی بودن ندارد.

الزام ۳-۴:

برنامه کاربردی پرداخت باید دسترسی به توابع / منابع مورد نیاز را محدود نموده و حداقل امتیاز را برای برای حساب‌های موجود در نظر بگیرد:

- به طور پیش فرض، تمام حساب‌های برنامه کاربردی / خدمات تنها به آن دسته از توابع / منابع دسترسی داشته باشند که برای هدف خاصی مورد نیاز است.
- به طور پیش فرض، تمام حساب‌های برنامه کاربردی / خدمات حداقل سطح امتیاز را برای هر تابع / منبع داده مورد نیاز داشته باشند.

معادل با الزام ۷ PCI DSS

٤) الزام ٤:

فعالیت‌های برنامه کاربردی پرداخت ثبت شود.

الزام ۴-۱:

در تکمیل فرآیند نصب، نصب "out of the box" پیش فرض برنامه بایستی تمام دسترسی‌های کاربر را وارد نموده و قادر به اتصال تمام فعالیت‌ها به کاربران شخصی باشد.

معادل با الزام ۱۰-۱ PCI DSS

الزام ۴-۲:

برنامه کاربردی پرداخت باید مسیرهای ممیزی خودکار جهت بازسازی وقایع زیر را ارائه نماید:

معادل با الزام ۱۰-۲ PCI DSS

الزام ۴-۲-۱: همه دسترسی‌های فردی کاربر به اطلاعات دارنده کارت از برنامه کاربردی

الزام ۴-۲-۲: همه اقدامات انجام شده توسط هر فرد با دسترسی مدیریتی و امتیازات مشخص شده در برنامه کاربردی

الزام ۴-۲-۳: دسترسی به برنامه‌های audit trail مدیریت شده در برنامه کاربردی

الزام ۴-۲-۴: تلاش‌های دسترسی منطقی نامعتبر

الزام ۴-۲-۵: استفاده و تغییرات مکانیسم شناسایی و احراز هویت برنامه (از جمله ایجاد حساب جدید، توسعه امتیازات، و غیره)، و تمام تغییرات، اضافات، حذفیات در حساب برنامه با دسترسی مدیریتی

الزام ۴-۲-۶: مقدار دهی اولیه، توقف یا مکث logهای audit

الزام ۴-۲-۷: ایجاد و حذف object در سطح سیستم در داخل و یا توسط برنامه

الزام ۴-۳:

برنامه کاربردی پرداخت باید حداقل موارد audit trail زیر را برای هر رویداد ثبت کند:

معادل با الزام ۱۰-۳ PCI DSS

الزام ۴-۳-۱: شناسایی کاربر

الزام ۴-۳-۲: نوع رویداد

الزام ۴-۳-۳: تاریخ و زمان

الزام ۴-۳-۴: شاخص موفقیت یا شکست

الزام ۴-۳-۵: منشاء رویداد

الزام ۴-۳-۶: هویت و یا نام داده تاثیرگذار، جزء سیستم، و یا منبع

الزام ۴-۴:

برنامه کاربردی پرداخت باید ورود به برنامه را به صورت متمرکز تسهیل کند.

معادل با الزام PCI DSS ۳-۵-۱۰

نکته: به عنوان مثال:

- ورود از طریق مکانیسم‌های فایل log استاندارد صنعت مانند سیستم فایل log مشترک (CLFS[1])، syslog، متن محدود، و غیره
- تبدیل فرمت ورود اختصاصی برنامه به فرمت ورود استاندارد صنعت جهت ورود سریع و متمرکز.

۵) الزام ۵:

برنامه‌های کاربردی پرداخت امن ایجاد شود.

الزام ۵-۱:

فروشنده نرم‌افزار باید یک فرایند رسمی برای توسعه امن برنامه‌های کاربردی پرداخت به شرح ذیل تعریف و اجرا نماید:

- توسعه برنامه‌های کاربردی پرداخت مطابق با PCI DSS و PA-DSS (برای مثال، احراز هویت و ورود امن)
- توسعه فرایندهای مبتنی بر استانداردها و یا best practiceهای صنعت
- ترکیب امنیت اطلاعات در کل طول چرخه حیات توسعه نرم‌افزار
- بررسی امنیتی قبل از انتشار برنامه یا آپدیت آن

معادل با الزام PCI DSS ۳-۶

الزام ۵-۱-۱: PANهای دایر برای تست و یا توسعه استفاده نشود.

[1] Common Log File System

معادل با الزام ۶-۴-۳ PCI DSS

الزام ۵-۱-۲: اطلاعات و حساب‌های آزمایشی قبل از انتشار به مشتری حذف شود.

معادل با الزام ۶-۴-۴ PCI DSS

الزام ۵-۱-۳: حساب‌های برنامه کاربردی پرداخت، IDهای کاربری، و کلمات عبور سفارشی از انتشار برنامه‌های کاربردی پرداخت حذف شود.

معادل با الزام ۶-۳-۱ PCI DSS

الزام ۵-۱-۴: کد برنامه کاربردی پرداخت قبل از عرضه به مشتریان بعد از هر تغییر مهم جهت شناسایی هر گونه آسیب‌پذیری برنامه نویسی بالقوه (با استفاده از فرآیندهای دستی یا خودکار و حداقل موارد زیر) بررسی شود:

- تغییرات کد توسط فرد دیگری غیر از نویسنده کد و افراد آگاه در تکنیک‌های کد و شیوه برنامه‌نویسی امن بررسی شود.
- در بررسی کد اطمینان حاصل شود که کد مطابق با دستورالعمل امن برنامه نویسی توسعه یافته است. (الزام ۵-۲ PA-DSS)
- اصلاحات مناسب قبل از انتشار اجرا شود.
- نتایج بررسی کد قبل از عرضه توسط مدیریت بررسی و تایید شود.
- نتایج بررسی کد شامل تایید مدیریت، نویسنده کد، بررسی کننده کد و اصلاحات قبل از عرضه مستند شود.

معادل با الزام ۶-۳-۲ PCI DSS

الزام ۵-۱-۵: شیوه‌های کنترل منبع امن به منظور بررسی یکپارچگی کد منبع در طول فرایند توسعه اجرا شود.

الزام ۵-۱-۶: برنامه‌های کاربردی پرداخت مطابق با best practiceهای صنعت برای تکنیک‌های برنامه نویسی امن، از جمله موارد زیر توسعه یابد:

- با حداقل امتیاز برای محیط برنامه
- با پیش فرض fail-safe (همه اجراها به طور پیش فرض رد شود مگر اینکه در طراحی اولیه مشخص شده باشد).
- برای تمامی نقاط دسترسی، از جمله انواع ورودی‌ها مانند ورودی چند کاناله به برنامه.

الزام ۵-۱-۶-۱: تکنیک‌های برنامه نویسی شامل مستندات PAN و / یا SAD در حافظه انجام می‌شود.

الزام ۵-۱-۷: ارائه آموزش در شیوه‌های توسعه امن برای توسعه دهندگان نرم‌افزار، برای مثال:

- طراحی برنامه امن
- تکنیک‌های برنامه نویسی امن برای جلوگیری از آسیب‌پذیری‌های رایج برنامه نویسی (به عنوان مثال، دستورالعمل فروشنده، ۱۰ OWASP برتر، ۲۵ SANS CWE برتر، برنامه نویسی امن CERT، و غیره)
- مدیریت اطلاعات حساس در حافظه
- بررسی کد
- تست امنیت (برای مثال، تکنیک‌های تست نفوذ)
- تکنیک‌های ارزیابی خطر.

الزام ۵-۱-۷-۱: تکنولوژی‌ها و روش‌های جدید در صورت نیاز آموزش داده شود.

الزام ۵-۲:

در فرآیندهای توسعه نرم‌افزار از آسیب‌پذیری‌های رایج برنامه نویسی پیش گیری شود.

معادل با الزام ۶-۵ PCI DSS

نکته: این آسیب‌پذیری‌ها در الزام ۵-۲-۱ الی ۵-۲-۱۰ PA-DSS و ۶-۵-۱ الی ۶-۵-۱۰ PCI DSS ذکر شده است.

الزام ۵-۲-۱: معایب تزریق، به خصوص SQL، همچنین OS Command، LDAP و XPath و غیره.

الزام ۵-۲-۲: سرریز بافر

الزام ۵-۲-۳: ذخیره رمزنگاری ناامن

الزام ۵-۲-۴: ارتباطات ناامن

الزام ۵-۲-۵: مدیریت نامناسب خطا

الزام ۵-۲-۶: تمام آسیب‌پذیری‌های "پر خطر" که در فرآیند شناسایی آسیب‌پذیری‌ها در الزام ۷-۱ PA-DSS شناسایی می‌شود.

نکته: الزامات ۵-۲-۷ الی ۵-۲-۱۰ برای برنامه‌های کاربردی مبتنی بر وب و رابط برنامه (داخلی یا خارجی) به کار می‌رود:

الزام ۵-۲-۷: Cross-Site Scripting (XSS)

الزام ۵-۲-۸: کنترل دسترسی نامناسب مانند مراجع object مستقیم ناامن، عدم محدودسازی دسترسی URL و پیمایش دایرکتوری)

الزام ۵-۲-۹: Cross-Site Request Forgery (CSRF)

الزام ۵-۲-۱۰: مدیریت جلسه و احراز هویت نقض شده

الزام ۵-۳:

فروشنده نرم‌افزار باید روش‌های کنترل تغییر را برای تمام تغییرات برنامه دنبال کند. روش کنترل تغییر باید همان مراحل توسعه نرم‌افزار را به عنوان نسخه‌های جدید دنبال کند (طبق الزام ۵-۱ PA-DSS) و شامل موارد زیر باشد:

معادل با الزام ۶-۴-۵ PCI DSS

الزام ۵-۳-۱: مستندات تاثیر

الزام ۵-۳-۲: مجوز مستند تغییر توسط احزاب مجاز مقتضی

الزام ۵-۳-۳: تست قابلیت به منظور بررسی عدم تاثیر نامطلوب تغییر بر روی امنیت سیستم

الزام ۵-۳-۴: روش لغو و یا حذف محصول

الزام ۵-۴:

فروشنده برنامه کاربردی پرداخت بایستی روش نسخه‌گذاری نرم‌افزار را به عنوان بخشی از چرخه حیات توسعه سیستم خود ثبت و دنبال کند. این روش باید مطابق با راهنمای برنامه PA-DSS و شامل حداقل موارد زیر باشد:

الزام ۵-۴-۱: روش نسخه‌گذاری باید المان‌هایی به شرح زیر داشته باشد:

- جزئیات چگونگی تطابق المان‌های طرح نسخه با الزامات مشخص شده در راهنمای برنامه PA-DSS.
- فرمت طرح نسخه، شامل تعداد المان‌ها، تفکیک کننده‌ها، مجموعه کاراکتر، و غیره (متشکل از حروف الفبا، اعداد، و / یا هردو).
- تعریف المان‌ها در طرح نسخه (برای مثال، نوع تغییر، انتشار بزرگ، کوچک، و یا تعمیر، wildcard، و غیره)
- تعریف عناصر که استفاده از wildcard را مشخص می‌نماید.

نکته: wildvardها ممکن است تنها برای المان‌های شماره نسخه ای که نشان‌دهنده تغییرات تأثیرگذار غیرامنیتی است، جایگزین شده باشد. برای الزامات استفاده از wildcardها به الزام ۵-۴-۳ مراجعه شود.

الزام ۵-۴-۲: روش نسخه‌گذاری باید نوع و اثرات همه تغییرات برنامه مطابق با راهنمای برنامه PA-DSS را نشان دهد، از جمله:

- شرح انواع و اثرات تغییرات برنامه.

- شناسایی و تعریف خاص تغییرات شامل:

  - تاثیری بر قابلیت‌های برنامه و یا وابستگی‌های آن نداشته باشد.
  - تاثیر بر قابلیت‌های برنامه داشته، اما هیچ تاثیری بر امنیت و یا الزامات PA-DSS ندارد.
  - بر روی قابلیت‌های امنیتی و الزامات PA-DSS تاثیر دارد.

- چگونگی ارتباط هر نوع از تغییرات با شماره نسخه خاص.

الزام ۵-۴-۳: روش نسخه‌گذاری بایستی استفاده wildcardها و چگونگی آن را که شامل موارد ذیل است، تشخیص دهد:

- جزئیات چگونگی استفاده از wildcardها در روش نسخه‌گذاری
- wildcardها برای تغییراتی که بر امنیت و یا الزامات PA-DSS تاثیر داشته، استفاده نشود.
- المانی از شماره نسخه که برای تغییرات فاقد تأثیر روی امنیت (از جمله المان wildcard) استفاده می‌شود، نباید برای تغییرات تاثیردار روی امنیت استفاده شود.
- المان‌های wildcard بایستی پس از المان‌های نسخه نشان دهنده تغییرات تأثیرگذار روی امنیت باشد.

نکته: wildcardها تنها مطابق با راهنمای برنامه PA-DSS استفاده می‌شود.

الزام ۵-۴-۴: روش نسخه‌گذاری منتشرشده توسط فروشنده باید به مشتریان و یکپارچه سازان / نمایندگان فروش ابلاغ شود.

الزام ۵-۴-۵: اگر یک نسخه داخلی به طرح نسخه‌گذاری منتشر شده نگاشت شود، روش نسخه‌گذاری باید نسخه داخلی را به نسخه خارجی نگاشت کند.

الزام ۵-۴-۶: فروشنده نرم‌افزار باید فرایند بررسی آپدیت برنامه جهت انطباق با روش نسخه‌گذاری قبل از انتشار داشته باشد.

الزام ۵-۵:

تکنیک‌های ارزیابی ریسک (برای مثال، مدل سازی تهدید) برای شناسایی معایب و آسیب‌پذیری امنیتی بالقوه در طول فرآیند توسعه نرم‌افزار استفاده شود. فرآیندهای ارزیابی ریسک شامل موارد زیر است:

- پوشش تمام توابع برنامه کاربردی پرداخت، از جمله ویژگی‌های تأثیرگذار بر امنیت و متقاطع با مرز اعتماد.
- ارزیابی نقاط تصمیم‌گیری، جریان فرآیند، جریان داده، ذخیره داده، و مرزهای اعتماد.
- تشخیص تمام نواحی متعامل با PAN و / یا SAD یا محیط اطلاعات دارنده کارت (CDE[1]) و همچنین تمام نتایج مبتنی بر فرآیند.
- لیستی از تهدیدات و آسیب‌پذیری بالقوه ناشی از آنالیز جریان اطلاعات دارنده کارت و اختصاص درجه ریسک برای هر یک از آنها (برای مثال، اولویت بالا، متوسط، و یا پایین).
- اجرای اصلاحات و اقدامات متقابل مناسب در طول فرایند توسعه.
- مستندسازی نتایج ارزیابی ریسک برای بررسی و تصویب مدیریتی.

الزام ۵-۶:

فروشنده نرم‌افزار باید فرایندی برای ثبت و اجازه انتشار نهایی برنامه و آپدیت آن پیاده‌سازی نماید. مستندات شامل موارد ذیل است:

- امضاء توسط یک بخش مجاز که به طور رسمی انتشار و یا آپدیت آن را تایید نماید.
- تایید فرایندهای توسعه امن که توسط فروشنده دنبال می‌شود.

۶) الزام ۶:

از انتقال بی‌سیم محافظت شود.

[1] Cardholder Data Environment

الزام ۶-۱:

برای برنامه‌های کاربردی پرداختی که از تکنولوژی‌های بی‌سیم استفاده می‌کنند، پیش‌فرض فروشنده‌های بی‌سیم تغییر داده شود، از جمله کلیدهای رمزگذاری بی‌سیم پیش فرض، کلمات عبور، و رشته عمومی SNMP. تکنولوژی‌های بی‌سیم باید به صورت امن اجرا شود.

معادل با الزام ۱-۲-۳ و ۲-۱-۱ PCI DSS

الزام ۶-۲:

برای برنامه‌های کاربردی پرداختی که از تکنولوژی‌های بی‌سیم استفاده می‌کنند، استفاده از best practiceها به منظور اجرای رمزنگاری قوی برای احراز هویت و انتقال تسهیل شود (برای مثال، IEEE 802.11i).

معادل با الزام ۴-۱-۱ PCI DSS

نکته: استفاده از WEP به عنوان یک کنترل امنیتی ممنوع است.

الزام ۶-۳:

دستورالعمل استفاده ایمن از تکنولوژی بی‌سیم برای مشتریان ارائه شود.

معادل با الزام ۱-۲-۳ و ۲-۱-۱ و ۴-۱-۱ PCI DSS

۷) الزام ۷:

برنامه‌های کاربردی پرداخت جهت شناسایی آسیب‌پذیری‌ها تست و آپدیت شود.

الزام ۷-۱:

فروشندگان نرم‌افزار باید یک فرایند شناسایی و مدیریت آسیب‌پذیری به شرح زیر ایجاد نمایند:

معادل با الزام ۶-۱ PCI DSS

الزام ۷-۱-۱: شناسایی آسیب‌پذیری‌های امنیتی جدید با استفاده از منابع معتبر برای به دست آوردن اطلاعات آسیب‌پذیری امنیتی.

الزام ۷-۱-۲: اختصاص درجه بندی ریسک برای همه آسیب‌پذیری‌های شناسایی شده، از جمله آسیب‌پذیری‌های مربوط به هر نرم‌افزار و یا سیستم‌های ارائه شده یا موردنیاز برنامه کاربردی پرداخت.

الزام ۷-۱-۳: تست وجود آسیب‌پذیری برنامه‌های کاربردی پرداخت و آپدیت آن قبل از عرضه.

الزام ۷-۲:

فروشندگان نرم‌افزار باید یک فرایند برای توسعه و استقرار به موقع patch وآپدیت‌های امنیتی ایجاد نمایند.

الزام ۷-۲-۱: patchها و آپدیت‌ها با شیوه ای امن و قابل اعتماد به مشتریان تحویل داده شود.

الزام ۷-۲-۲: patchها و آپدیت‌ها با حفظ یکپارچگی کد آن به مشتریان تحویل داده شود.

الزام ۷-۳:

یادداشت‌های انتشار آپدیت برنامه شامل مواردی از جمله جزئیات و تاثیر آپدیت باشد.

۸) الزام ۸:

اجرای شبکه امن تسهیل گردد.

الزام ۸-۱:

برنامه کاربردی پرداخت باید قادر به اجرا در یک محیط شبکه امن باشد. برنامه نباید مانع استفاده از دستگاه‌ها، برنامه‌های کاربردی، و یا تنظیمات مورد نیاز برای انطباق PCI DSS شود.

به عنوان مثال، برنامه نباید مانع نصب patch، حفاظت ضد بدافزار، تنظیمات فایروال، یا هر دستگاه، برنامه، یا پیکربندی مورد نیاز برای انطباق PCI DSS شود.

معادل با الزام ۱، ۳، ۴، ۵ و۶ PCI DSS

الزام ۸-۲:

برنامه کاربردی پرداخت بایستی فقط برای سرویس‌ها، پروتکل‌ها، daemonها، اجزا و نرم‌افزار و سخت افزار وابسته‌ی امن و ضروری استفاده شود.

برای مثال، اگر NetBIOS، اشتراک گذاری فایل، Telnet، FTP، و غیره، مورد نیاز برنامه باشد باید از طریق SSH، S-FTP، TLS، IPSec، و یا تکنولوژی‌های دیگر امن شود.

معادل با الزام ۲-۲-۳ PCI DSS

نکته: SSL و TLS اولیه رمزنگاری قوی ندارند. برنامه‌های کاربردی پرداخت نباید از آنها استفاده کند. برنامه‌هایی که از TLS پشتیبانی می‌نمایند نباید مجددا از SSL استفاده نمایند.

الزام ۸-۳:

برنامه کاربردی پرداخت نباید از سرویس‌ها و یا پروتکل‌هایی که مانع و یا متداخل با عملکرد طبیعی تکنولوژی احراز هویت دوعامله برای تامین امنیت دسترسی از راه دور به برنامه پرداخت در خارج از محیط مشتری است، استفاده نماید.

معادل با الزام ۸-۳ PCI DSS

نکته: احراز هویت دوعامله مستلزم استفاده از دو روش از میان سه روش احراز هویت (به شرح ذیل) است. استفاده دو مرتبه از یک عامل (به عنوان مثال، استفاده از دو کلمه عبور جداگانه) احراز هویت دوعامله محسوب نمی‌شود. روش‌ها و یا عامل‌های احراز هویت، عبارتند از:

- آنچه که شما می‌دانید، مانند یک رمز یا عبارت عبور،

- آنچه که شما دارید، مانند یک دستگاه توکن یا کارت هوشمند،
- آنچه که شما هستید، مانند یک بیومتریک، مشخصات فیزیکی یا رفتاری.

نمونه ای از تکنولوژی دوعامله عبارتند از RADIUS با توکن، TACACS با توکن، و غیره.

۹) الزام ۹:

اطلاعات دارنده کارت نباید هرگز در سرور متصل به اینترنت ذخیره شود.

الزام ۹-۱:

برنامه کاربردی پرداخت باید به طوری توسعه یابد که هر وب سرور و هر جزء ذخیره‌سازی اطلاعات دارنده کارت (برای مثال، یک سرور پایگاه داده) نیازی به بودن روی همان سرور و همان منطقه شبکه (مانند یک DMZ) با وب سرور نداشته باشد.

معادل با الزام ۱-۳-۷ PCI DSS

۱۰) الزام ۱۰:

دسترسی امن از راه دور به برنامه کاربردی پرداخت تسهیل شود.

الزام ۱۰-۱:

احراز هویت دوعامله باید برای همه دسترسی‌های از راه دور به برنامه که از خارج از محیط مشتری سرچشمه می‌گیرد، استفاده شود.

معادل با الزام ۸-۳ PCI DSS

الزام ۱۰-۲:

هر گونه دسترسی از راه دور به برنامه باید به شرح زیر ایمن انجام شود:

الزام ۱۰-۲-۱: اگر آپدیت برنامه از طریق دسترسی از راه دور به سیستم‌های مشتریان تحویل داده شود، فروشندگان نرم‌افزار باید روشن نمودن تکنولوژی‌های دسترسی از راه دور

را تنها در زمان دانلود از فروشنده، و خاموش کردن بلافاصله پس از تکمیل دانلود را به مشتریان بیان نمایند.

همچنین، اگر از طریق شبکه‌های خصوصی مجازی (VPN) و یا دیگر اتصالات با سرعت بالا باشد، فروشندگان نرم‌افزار باید پیکربندی درست یک فایروال یا یک محصول فایروال شخصی را جهت امنیت بخشیدن به اتصالات همیشه روشن به مشتریان توصیه نمایند.

معادل با الزام ۱ و ۱۲-۳-۹ PCI DSS

الزام ۱۰-۲-۲: اگر فروشندگان و یا یکپارچه سازان / نمایندگان فروش بتوانند به برنامه‌های کاربردی پرداخت مشتریان از راه دور دسترسی داشته باشند، بایستی یک اعتبارنامه احراز هویت منحصر به فرد (مانند یک کلمه عبور / عبارت عبور) برای هر یک از مشتریان استفاده شود.

معادل با الزام ۸-۵-۱ PCI DSS

الزام ۱۰-۲-۳: دسترسی از راه دور به برنامه‌های کاربردی پرداخت مشتریان توسط فروشندگان و یا یکپارچه سازان / نمایندگان فروش، و یا مشتریان باید به صورت امن اجرا شود، برای مثال:

- تنظیمات پیش‌فرض نرم‌افزار دسترسی از راه دور تغییر یابد. (برای مثال، کلمه عبور پیش فرض را تغییر داده و از کلمات عبور منحصر به فرد برای هر یک از مشتریان استفاده شود).
- تنها به آدرس‌های MAC / IP خاص (شناخته شده) اجازه اتصال داده شود.
- از احراز هویت قوی و کلمات عبور پیچیده برای ورود استفاده شود. (مطابق با الزامات۳-۱-۱ الی ۳-۱-۱۱ PA-DSS).
- انتقال داده‌های رمزگذاری شده مطابق با الزام ۱۲-۱ PA-DSS فعال شود.

- حساب پس از تعداد معینی از ورود ناموفق قفل شود. (مطابق با الزامات ۳-۱-۹ و ۳-۱-۱۰ PA-DSS)
- یک اتصال VPN قبل از اجازه دسترسی از طریق یک فایروال برقرار گردد.
- یک تابع ورود به سیستم فعال شود.
- دسترسی به محیط مشتری توسط پرسنل یکپارچه سازان / نمایندگان فروش محدود گردد.

معادل با الزام ۲، ۸ و ۱۰ PCI DSS

۱۱) الزام ۱۱:

ترافیک حساس بر روی شبکه‌های عمومی رمزگذاری گردد.

الزام ۱۱-۱:

اگر برنامه کاربردی پرداخت اطلاعات دارنده کارت را از طریق شبکه‌های عمومی ارسال کند، باید از پروتکل‌های رمزنگاری و امنیت قوی (برای مثال، TLS، IPSEC، SSH، و غیره) که حداقل شامل موارد ذیل می‌باشد، برای حفاظت از اطلاعات حساس دارنده کارت در زمان انتقال در شبکه‌های عمومی و باز استفاده کند:

- فقط کلیدها و گواهی‌های معتبر و مورد اعتماد پذیرفته شود.
- پروتکل فقط برای پشتیبانی از نسخه‌ها و یا تنظیمات امن استفاده شود.
- قدرت رمزگذاری برای روش رمزگذاری استفاده شده مناسب باشد.

معادل با الزام ۴-۱ PCI DSS

نکته: نمونه‌هایی از شبکه عمومی و باز شامل موارد زیر می‌باشد:

- اینترنت
- تکنولوژی‌های بی سیم، از جمله بلوتوث و 802.11
- تکنولوژی‌های سلولی، برای مثال، سیستم جهانی برای ارتباطات موبایل (GSM)، دسترسی چندگانه تقسیم کد (CDMA)
- خدمات رادیویی بسته‌ای عمومی (GPRS)

الزام ۱۱-۲:

اگر برنامه کاربردی پرداخت PANها را از طریق تکنولوژی پیام‌رسانی کاربر نهایی (برای مثال، ایمیل، پیام‌های فوری، چت) ارسال کند، باید یک راهکار برای ناخوانا نمودن PAN و رمزگذاری قوی آن ارائه نماید.

۱۲) الزام ۱۲:

تمام دسترسی‌های مدیریتی غیرکنسول رمزگذاری شود.

معادل با الزام PCI DSS ۲-۴

الزام ۱۲-۱:

در صورت ارائه مدیریت مبتنی بر وب و یا سایر دسترسی‌های مدیریتی غیرکنسول، بایستی همه دسترسی‌ها با تکنولوژی‌هایی مانند SSH، VPN یا TLS رمزگذاری شود.

معادل با الزام PCI DSS ۲-۳

نکته: پروتکل‌های clear-text مانند Telnet یا rlogin نباید برای دسترسی‌های مدیریتی استفاده شود.

الزام ۱۲-۲:

رمزنگاری قوی مبتنی بر وب و یا سایر دسترسی‌های مدیریتی غیرکنسول با استفاده از تکنولوژی‌هایی مانند SSH، VPN، و یا TLS به مشتریان آموزش داده شود.

معادل با الزام PCI DSS ۲-۳

۱۳) الزام ۱۳:

الزامات پیاده‌سازی PA-DSS برای مشتریان، فروشندگان و یکپارچه سازان ارائه شود.

الزام ۱۳-۱:

توسعه، نگهداری و انتشار راهنمای پیاده‌سازی PA-DSS برای مشتریان، نمایندگان فروش، و یکپارچه سازان به شرح زیر انجام شود:

الزام ۱۳-۱-۱: اطلاعات خاص مربوط به برنامه فراهم گردد.

الزام ۱۳-۱-۲: راهنمای پیاده‌سازی تمام الزامات PA-DSS ارائه شود.

الزام ۱۳-۱-۳: تغییرات برنامه و تاثیر آن بر الزامات PA-DSS حداقل سالانه بررسی شود.

۱٤) الزام ۱٤:

مسئولیت‌های PA-DSS برای پرسنل اختصاص یافته، و برنامه‌های آموزشی برای پرسنل، مشتریان، نمایندگان فروش و یکپارچه سازان ارائه گردد.

الزام ۱۴-۱:

امنیت اطلاعات و PA-DSS برای پرسنل دارای مسئولیت PA-DSS فروشندگان حداقل سالانه آموزش داده شود.

الزام ۱۴-۲:

نقش‌ها و مسئولیت‌های PA-DSS به شرح ذیل برای پرسنل اختصاص یابد:

- مسئولیت کلی در برابر الزامات PA-DSS
- حفظ آپدیت‌ها در طی تغییرات راهنمای برنامه PCI SSC PA-DSS
- حصول اطمینان از برنامه نویسی
- حصول اطمینان از آموزش و پشتیبانی نمایندگان فروش و یکپارچه‌سازان
- حصول اطمینان از آموزش تمام پرسنل دارای مسئولیت PA-DSS فروشندگان، از جمله توسعه‌دهندگان.

الزام ۱۴-۳:

برنامه‌های آموزشی و ارتباطی برای نمایندگان فروش و یکپارچه سازان برنامه کاربردی پرداخت توسعه و پیاده‌سازی گردد، که حداقل شامل موارد زیر باشد:

- چگونگی پیاده‌سازی سیستم‌های برنامه کاربردی پرداخت و مرتبط و شبکه مطابق با PCI DSS

- پوشش همه موارد راهنمای پیاده‌سازی PA-DSS

الزام ۱۴-۳-۱: موارد آموزشی با توجه به الزامات PA-DSS و تغییرات برنامه حداقل سالانه نقد و بررسی و آپدیت شود.

فصل ٤

امنیت تراکنش احراز هویت PCI PTS
(PIN Transaction Security)

مقدمه

PTS مخفف PIN Transaction Security و استاندارد امنیت تراکنش احراز هویت بوده و از اولویت‌های استراتژیک PCI محسوب می‌شود و هدف اصلی آن حفاظت از PINمی‌باشد.

در این خصوص سه نوع دستگاه مورد نظر می‌باشد:

- PED (PIN Entry Device)، شامل انواع ترمینال‌هایی که توسط پذیرنده‌ها جهت تراکنش‌های کارت استفاده می‌گردد.

- EPP (Encrypting PIN PAD)، بخشی از پایانه‌ها از نوع غیرحضوری مانند ATM (Automated Teller Machine) که جهت ورود از رمز استفاده می‌گردد.
- اجزاء امن پایانه‌های فروش مانند کارتخوان‌های امن و دستگاه‌های مربوط به ورود رمز دارنده کارت می‌باشد.

در PTS خصوصیات فیزیکی و قابلیت دستگاه‌های ورود رمز دارنده کارت مشخص شده است.

در این استاندارد نیازمندی‌های این تجهیزات و داده‌های لازم برای این استاندارد، روش تست و مراحل دریافت و تاییدیه تعریف شده است. بر اساس این مشخصات، دستگاه می-بایست نفوذ فیزیکی (attack) و نفوذ برای دستیابی به کلیدهای ذخیره شده در دستگاه را تشخیص دهد.

این مهم در کل چرخه حیات دستگاه از تولید تا بکارگیری آن می‌بایست قابل کنترل باشد و به خوبی مدیریت گردد.

وجود این استاندارد باعث تسریع در توسعه فناوری پرداخت شده است. در گذشته فروشندگان این گونه تجهیزات نیاز به انجام تست‌های اختصاصی در آزمایشگاه‌ها داشتند که وقت‌گیر و پرهزینه بوده است. اما با ایجاد استانداردهای امنیتی بین‌المللی قدم موثری در کاهش هزینه و پیچیدگی‌های تراکنش‌های پرداخت کارت برداشته شده است.

از جمله شرکت‌های معتبری که در کمیته طراحان این استاندارد فعالیت داشته‌اند JCB، Visa و MasterCard می‌باشند.

در این استاندارد امنیت PIN با ترکیبی از امنیت فیزیکی و منطقی تامین خواهد شد.

به طور خلاصه پایانه‌ها از نظر فیزیکی می‌بایست ویژگی‌های زیر را داشته باشند:

- Tamper detection: این دستگاه‌ها از مکانیزم‌هایی مانند Secure box، Zebra connector جهت تشخیص Tampering استفاده می‌کنند.

- با تشخیص دستکاری دستگاه، کلیه اطلاعات مربوط به کلیدهای بارگذاری شده آن حذف گردد.
- Tamper evidence: این دستگاه‌ها با نمایش وضعیت Tampering اجازه انجام عملیات را نمی‌دهند.
- تنها با ابزارهایی خاص امکان برگرداندن این دستگاه‌ها به حالت عملیاتی وجود خواهد داشت.

همچنین پایانه‌ها از نظر منطقی می‌بایست ویژگی‌های زیر را داشته باشند:

- هر نرم‌افزاری که بر امنیت اثرگذار می‌باشد لازم است قبل از بارگذاری، احراز هویت شود.
- رابط‌های کاربری برای ورود رمز می‌بایست کاملا واضح باشند و باعث سردرگمی مشتری نگردد. لذا در برخی پایانه‌ها این بخش از نرم‌افزار می‌بایست احرازهویت گردند.
- پایانه می‌بایست از الگوریتم‌های رمزنگاری برای احرازهویت به صورت online پشتیبانی نماید.
- پایانه می‌بایست از متدهای پروتکل EMV برای احرازهویت به صورت offline پشتیبانی نماید.

مدیریت PIN :

نیازهای امنیتی در ورود رمز کارت:

- وجود حفاظ برای مخفی نگاه داشتن کلیدهای وارد شده در پایانه.
- راهنمایی صحیح و واضح به مشتری هنگام ورود رمز کارت.
- حفاظت در مقابل پایش صوت، تشعشعات الکترومغناطیس و مصرف برق برای کشف رمز کارت.
- سازگاری با استاندارد ISO 9564-1، این استاندارد حداقل نیازمندی‌ها را در online PIN بیان می‌کند.

روش‌های صحت‌سنجی رمز مشتری:

:Online PIN verification

در این روش صحت شماره رمز مشتری به صورت online و توسط سوییچ کارت کنترل می‌گردد که مرتبط با کارت‌های مغناطیسی و هوشمند می‌باشد.

نحوه انتقال رمز و محدودیت‌های موردنیاز به شرح ذیل می‌باشد:

- استفاده از کلیدهای متقارن با الگوریتم‌های DES/3DES در تولید کلید Session
- استفاده از کلیدهای متقارن DES و 3DES در روش DUKPT (Drive Unique Key Per Transaction)
- بارگذاری کلید به صورت امن
- عدم تشابه کلیدها
- عدم دسترسی برنامه به رمز وارد شده توسط مشتری
- پشتیبانی از استاندارد ISO 9564-2، در این استاندارد الگوریتم‌های رمزنگاری PIN (Personal Identification Number) تعریف شده است.

:Offline PIN verification

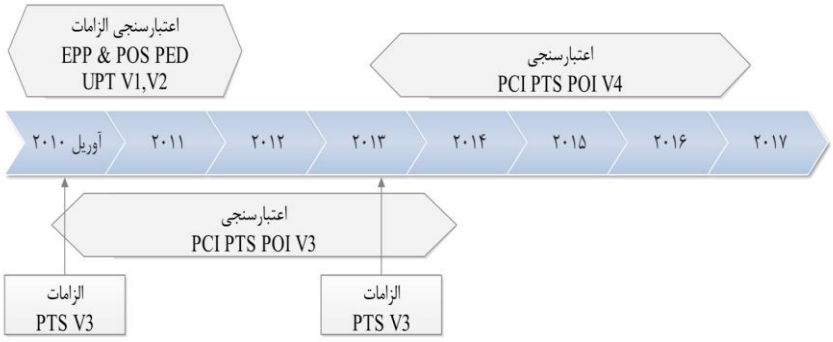
در این روش صحت شماره رمز مشتری به صورت offline توسط کارت هوشمند کنترل می‌گردد. تبادل کلید بین پایانه و کارت به صورت‌های زیر می‌تواند باشد:

- بررسی صحت شماره رمز با ارسال PIN وارد شده به کارت
- بررسی صحت شماره رمز با ارسال PIN رمز شده به کارت
- استفاده از تولید کننده شماره تصادفی مطابق با NIST 800-22
- عدم دسترسی برنامه به رمز وارد شده توسط مشتری
  - رمز باید در PED وارد شده باشد.
  - PIN برای کنترل به کارت ارسال گردد.

پایه و اساس کار این استاندارد افزایش کنترل‌ها روی داده می‌باشد و در تمام بخش‌هایی که اطلاعات دارنده کارت را نگهداری و پردازش و تبادل می‌کنند، قابل استفاده است.

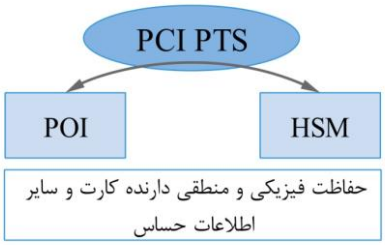
انواع دستگاه‌ها:

نمودار زیر الزامات امنیتی نسخه‌های مختلف این استاندارد را نشان می‌دهد:



شکل ۴-۱: نسخه‌های استاندارد PCI PTS

هدف این استاندارد حفاظت منطقی و یا فیزیکی دارنده کارت و یا سایر اطلاعات حساس در دستگاه‌های نقطه تعامل (POI[1]) و ماژول‌های امنیتی سخت‌افزار (HSM[2]) به شکل زیر است:



شکل ۴-۲: دستگاه‌های PTS

[1] Point Of Interaction
[2] Hardware Security Module

POI: یک محصول پذیرش تراکنش الکترونیکی است. یک POI متشکل از سخت‌افزار و نرم‌افزار و تجهیزات پذیرش تراکنش کارت دارنده کارت است. POI ممکن است بامراقب[1] یا بی‌مراقب[2] باشد. تراکنش‌های POI شامل تراکنش‌های مبتنی بر کارت IC، نوار مغناطیسی، و غیرتماسی است.

HSM: یک دستگاه سخت‌افزاری فیزیکی و منطقی محافظت‌شده است که مجموعه‌ای امن از خدمات رمزنگاری را فراهم می‌کند. این دستگاه شامل مجموعه‌ای از سخت‌افزار، سیستم عامل (نرم‌افزار دائمی)، نرم‌افزار، و یا ترکیبی از آنها است که منطق رمزنگاری، فرآیندهای رمزنگاری و یا هر دوی آنها از جمله الگوریتم‌های رمزنگاری را پیاده‌سازی می‌کند.

الزامات استاندارد PCI PTS POI

الزامات امنیتی این استاندارد در دستگاه‌های POI (PCI PTS POI) به ۵ گروه به شرح جدول زیر تقسیم می‌شود:

جدول ۴-۱: الزامات PCI PTS POI

ماژول الزامات و ارزیابی	توصیف
الزامات اصلی دستگاه POI	الزامات اصلی منطقی و فیزیکی دستگاه‌های پذیرش PIN
یکپارچه‌سازی پایانه POS	الزامات مدیریت امنیتی قابل اجرا در دستگاه‌های یکپارچه
پروتکل‌های باز (OP[3])	رابط پایانه‌های POI با شبکه‌های باز با استفاده از پروتکل‌های باز
خواندن و تبادل امن اطلاعات (SRED[4])	برای پشتیبانی از رمزنگاری امن از داده‌های حساب کاربری در POI
الزامات امنیتی مدیریت دستگاه	چگونگی تولید، کنترل، ارسال، ذخیره و استفاده در طول چرخه حیات

[1] Attended
[2] Unattended
[3] Open Protocols
[4] Secure Reading and Exchange of Data

- دو ماژول اول در نسخه‌های قبلی PCI PED, EPP, & UPT نیز وجود داشت.
- هر محصولی که شامل ماژول‌های جداگانه باشد – مانند EPP، ریدر کارت، غیره – بایستی الزامات یکپارچه‌سازی را رعایت نماید.
- محصولات ملزم به پشتیبانی از پروتکل‌های باز و یا SRED نیستند؛ اما در صورت پشتیبانی از آنها بایستی الزامات آن رعایت گردد.
- در ماژول‌های الزامات اصلی و یکپارچه‌سازی پایانه موارد زیر مورد ارزیابی قرار می‌گیرد:

جدول ۴-۲: موارد ارزیابی در ماژول‌های الزامات اصلی و یکپارچه‌سازی

پشتیبانی PIN	N/A
	فقط آفلاین
	آفلاین و آنلاین
	فقط آنلاین
مدیریت کلید	N/A
	DUKPT
	Fixed
	MK/SK
تکنولوژی ورود PIN	N/A
	کلیدهای فیزیکی (سخت)
	صفحه لمسی
	سایر
کنترل پیام اعلان	N/A
	کنترل پذیرنده
	کنترل سازنده پایانه
	سایر
سایر قابلیت‌های ارائه شده	نمایش
	CTLS
	ICCR
	MSR
	OP
	SRED

- در ماژول پروتکل باز موارد زیر مورد ارزیابی قرار می‌گیرد:

جدول ۴-۳: موارد ارزیابی در ماژول پروتکل باز

	بله	خیر	N/A	نام	شماره
پروتکل‌های لایه ارتباط					
پروتکل‌های IP					
پروتکل‌های امنیتی					
سرویس‌های IP					
استفاده از SRED					

۱) ماژول ۱: الزامات اصلی

الزام A: الزامات امنیتی اصلی فیزیکی

الزام A1: این دستگاه از مکانیسم‌های تشخیص و پاسخ Tamper استفاده می‌کند که باعث از کار افتادن بلافاصله آن و در نتیجه پاک شدن اتوماتیک و فوری اطلاعات حساس ذخیره شده در دستگاه می‌شود، به طوری که غیرقابل بازیابی می‌گردد. این مکانیسم از دستگاه در برابر نفوذ فیزیکی از طریق دریل، لیزر، حلال‌های شیمیایی، کاورهای دهانه، کاور شکاف (درز) و دهانه تهویه محافظت می‌نماید، و به هیچ وجه قابلیت غیرفعال نمودن و یا شکست نداشته و مشکل افشای PIN و یا دسترسی به اطلاعات محرمانه بدون نیاز به حداقل پتانسیل حمله ۲۶ به ازای هر دستگاه برای شناسایی و بهره‌برداری اولیه، با حداقل ۱۳ برای بهره‌برداری، انحصاراً برای ریدر کارت IC وجود ندارد[۱].

نکته: جایگزینی جلو و عقب و پوشش باید به عنوان بخشی از هر سناریوی حمله در نظر گرفته شود. تمام حملات باید شامل حداقل زمان حمله ده ساعت برای بهره‌برداری باشد.

[۱] نحوه محاسبه پتانسیل حمله در پیوست ۱ مشخص گردیده است.

الزام A2: شکست یکی از مکانیزم‌های امنیتی تک، دلیل عدم تطبیق امنیت دستگاه نیست. حفاظت در مقابل یک تهدید بر اساس ترکیبی از حداقل دو مکانیزم امنیتی مستقل است.

الزام A3: امنیت دستگاه با تغییر شرایط محیطی و شرایط عملیاتی در معرض خطر نباشد. (مثلاً تغییرات دما یا ولتاژ)

الزام A4: توابع و یا داده‌های حساس فقط در مناطق حفاظت شده این دستگاه استفاده می‌شوند. اطلاعات و توابع حساس یعنی داده‌های حساسی که در برابر تغییرات، بدون نیاز به حداقل پتانسیل حمله ۲۶ برای شناسایی و بهره‌برداری اولیه، حداقل ۱۳ برای بهره‌برداری، انحصاراً برای ریدر کارت IC، برای شناسایی و بهره‌برداری اولیه محافظت شده است.

الزام A5: هیچ راه عملی برای تعیین ارقام PINای که وارد شده و به صورت داخلی منتقل می‌شود، توسط صدای مانیتورینگ، انتشار الکترومغناطیسی، مصرف برق و یا سایر ویژگی‌های بیرونی در دسترس مانیتورینگ (حتی با همکاری اپراتور دستگاه و یا کارمند فروش) بدون نیاز به یک حداقل پتانسیل حمله ۲۶ برای شناسایی و بهره‌برداری اولیه با حداقل ۱۳ برای بهره‌برداری وجود ندارد.

الزام A6: تعیین هر کلید رمزنگاری مربوط به امنیت PIN موجود در این دستگاه، توسط نفوذ و / یا مانیتورینگ دستگاه (از جمله نوسانات برق)، به حداقل پتانسیل حمله ۳۵ برای شناسایی و بهره‌برداری اولیه با حداقل ۱۵ برای بهره‌برداری نیاز دارد.

نکته: اگر دستگاه POI یک صفحه کلید دارد که می‌تواند برای ورود داده‌های غیر از PIN مورد استفاده قرار گیرد، حداقل بایستی یکی از موارد A7، B16 یا E3.4 را تامین کند: A7 برای اجزا و مسیرهای حاوی سیگنال‌های نمایش متن بین پردازنده رمزنگاری و واحد نمایش به کار می‌رود، B16 برای دستگاه‌هایی است که از رمزنگاری برای ارتباط با واحد نمایش استفاده یا آن را آپدیت می‌نمایند، (توسط فروشنده یا پذیرنده انجام می‌شود)، E3.4 برای دستگاه‌های بدون مراقبتی که جزو موارد فوق‌الذکر نمی‌باشد.

الزام A7: تغییر غیرمجاز درخواست ورود اطلاعات غیر PIN در صفحه کلید ورود PIN به طوری که PIN به خطر بیافتد، به عنوان مثال، درخواست ورود PIN هنگامی که خروجی رمزگذاری نشده است، نمی‌تواند بدون نیاز به حداقل پتانسیل حمله ۱۸ به ازای هر دستگاه برای شناسایی و بهره‌برداری اولیه با حداقل ۹ برای بهره‌برداری رخ دهد.

الزام A8: دستگاه وسیله‌ای را برای جلوگیری از مشاهده بصری ارزش PIN که توسط دارنده کارت وارد می‌شود فراهم نماید.

الزام A9: نفوذ به دستگاه به منظور ایجاد هرگونه اضافات، تعویض، و یا تغییرات ریدر کارت مغناطیسی و سخت‌افزار و یا نرم‌افزار مربوطه، به منظور تعیین و یا تغییر داده‌های مسیر مغناطیسی، بدون نیاز به حداقل پتانسیل حمله ۱۶ به ازای هر دستگاه، برای شناسایی و بهره‌برداری اولیه، با حداقل ۸ برای بهره‌برداری ممکن نیست.

الزام A10: برای دستگاه‌های بدون مراقبت، قطعات امن شامل یک مکانیسم ضد حذف برای محافظت در برابر حذف غیرمجاز و / یا نصب مجدد غیرمجاز درنظر گرفته شود. شکست یا دور زدن این مکانیسم بایستی با حداقل پتانسیل حمله ۱۸ به ازای هر دستگاه برای شناسایی و بهره‌برداری اولیه با حداقل ۹ برای بهره‌برداری باشد.

الزام A11: اگر ورود PIN با صداهای قابل شنیدن همراه باشد، آهنگ صدای هر کدام از ارقام PIN غیرقابل تشخیص از همدیگر باشد.

الزام B: الزامات امنیتی اصلی منطقی

الزام B1: دستگاه یک خود-آزمون، که شامل آزمون یکپارچگی و صحت پس از راه-اندازی و حداقل یک بار در روز برای بررسی حالت خطر دستگاه انجام دهد. در صورت شکست، دستگاه و قابلیت‌های آن به شیوه ای امن از کار بیافتد. حافظه دستگاه باید حداقل هر ۲۴ ساعت مقداردهی اولیه شود.

الزام B2: قابلیت دستگاه نباید توسط ناهنجاری‌های منطقی از جمله توالی دستور غیرمنتظره، دستورات ناشناخته، دستوراتی در حالت نادرست دستگاه و تامین پارامتر و یا

داده‌های نادرست که بتواند باعث ایجاد خروجی متن واضح PIN و یا سایر داده‌های حساس در دستگاه شود، تحت تاثیر قرار گیرد.

الزام B3: سیستم عامل و هرگونه تغییرات بعدی بازرسی و با استفاده از فرایند ممیزی و مستند بررسی شده و در برابر قابلیت‌های پنهان وغیرمجاز و یا غیرمستند تضمین شود.

الزام B4: اگر دستگاه امکان آپدیت سیستم عامل را داشته باشد بایستی به صورت رمزنگاری شده آن را احراز هویت نموده و در صورت عدم تایید رد و حذف شود.

الزام B4-1: سیستم عامل باید صحت تمام برنامه‌های کاربردی بارگذاری شده بر روی پایانه را مطابق با B4 تایید کند. اگر دستگاه امکان آپدیت برنامه کاربردی و یا تنظیمات نرم-افزار را داشته باشد بایستی به صورت رمزنگاری شده آن را مطابق با B4 احراز هویت نماید.

الزام B4-2: فروشنده باید یک فرآیند مستند حاوی جزئیات خاص در مورد چگونگی امضای مکانیزم قابل اجرا در سیستم‌های مدیریت اعلان نمایش و هر مکانیزم مورد استفاده برای احراز هویت کد نرم‌افزار فراهم کند.

- فرآیند امضا تحت کنترل دوگانه انجام شود.
- تمام فایل‌های اجرایی امضا شود.
- نرم‌افزار تنها با استفاده از یک دستگاه امن رمزنگاری ارائه شده توسط فروشنده پایانه امضا شود.

الزام B5: دستگاه نباید هرگز PIN واردشده را نمایش دهد. با سمبل‌هایی مانند ستاره نمایش داده شود.

الزام B6: اطلاعات حساس نباید به مدت طولانی حفظ و یا بیشتر از حد لازم استفاده شود. PIN آنلاین بلافاصله پس از ورود و تایید دارنده کارت مثلا با فشار دادن دکمه در داخل دستگاه رمزگذاری می‌شود.

دستگاه باید به طور خودکار بافر داخلی خود را در زمان‌های اتمام تراکنش و اتمام زمان انتظار پاسخ از سوی دارنده کارت و یا پذیرنده پاک کند.

الزام B7: دسترسی به سرویس‌های حساس نیاز به احراز هویت داشته باشد. سرویس-های حساس زمینه دسترسی به قابلیت‌های حساس را فراهم می‌کند. قابلیت‌های حساس همان پردازش داده‌های حساس مانند کلیدهای رمزنگاری، PIN، و کلمه عبور می‌باشد. ورود یا خروج سرویس‌های حساس نباید آشکار شده و یا بر داده‌های حساس تاثیر گذارد.

الزام B8: برای به حداقل رساندن خطرات ناشی از استفاده غیرمجاز از سرویس‌های حساس، در تعداد دفعات اقدامات و زمان محدودیت اعمال شود، تا دستگاه مجبور به بازگشت به حالت عادی خود شود.

الزام B9: اگر اعداد تصادفی مرتبط با امنیت اطلاعات حساس توسط دستگاه تولید شود، مولد عدد تصادفی جهت اطمینان از غیرقابل پیش‌بینی بودن اعداد بایستی ارزیابی شود.

الزام B10: این دستگاه دارای ویژگی پیشگیری و یا جلوگیری از تعیین جامع PIN است.

الزام B11: تکنیک‌های مدیریت کلید، مطابق با ISO 11568 و / یا ANSI X9.24 پیاده‌سازی شود. تکنیک‌های مدیریت کلید، باید از روش استخراج کلید ANSI TR-31 و یا یک روش معادل برای حفظ باندل کلید TDEA پشتیبانی کند.

الزام B12: تکنیک رمزگذاری PIN بر اساس تکنیک موجود در ISO 9564 اجرا شود.

الزام B13: رمزگذاری یا رمزگشایی هر داده دلخواه با استفاده از کلید رمزنگاری PIN و یا کلید رمزنگاری کلید امکان‌پذیر نباشد. دستگاه بایستی از مقادیر متفاوت برای کلیدهای داده‌های اختیاری، کلیدهای رمزنگاری کلید و کلیدهای رمزنگاری PIN استفاده کند.

الزام B14: هیچ مکانیزمی جهت خروج متن خصوصی و یا PIN، افشای رمزنگاری یک کلید یا PIN تحت یک کلید و یا انتقال متن واضح کلید از یک قسمت با امنیت بالا به یک قسمت با امنیت پایین‌تر در دستگاه وجود ندارد.

الزام B15: فرآیند ورود PIN باید از فرآیند ورود سایر اطلاعات تراکنش جهت اجتناب از نمایش تصادفی PIN بر روی صفحه نمایش دستگاه جدا باشد. اگر ورود PIN و سایر داده‌ها از طریق یک صفحه کلید باشد، باید عملیات ورود آنها جدا از یکدیگر باشد.

الزام B16: ورود تمام اطلاعات غیر PIN تحت کنترل واحد رمزنگاری دستگاه می‌باشد. اگر در داخل واحد رمزنگاری ذخیره شوند، نمی‌توانند بدون پاک شدن کلیدهای رمزنگاری واحد تغییر داده شوند. اگر در خارج از واحد رمزنگاری ذخیره شوند، مکانیسم‌های رمزنگاری جهت اطمینان از صحت و استفاده مناسب و جلوگیری از تغییر و استفاده نادرست باید وجود داشته باشد.

الزام B17: اگر دستگاه از نرم‌افزارهای متعدد پشتیبانی کند، باید آنها را تفکیک کند. نباید امکان تداخل و یا دستکاری با برنامه دیگر و یا سیستم عامل را داشته باشد، مثلا تغییر موضوع داده‌های متعلق به برنامه دیگر و یا سیستم عامل.

الزام B18: سیستم عامل این دستگاه باید شامل نرم‌افزار (قطعات و خدمات) لازم برای عملکرد مدنظر باشد. سیستم عامل باید به صورت امن پیکربندی و با حداقل امتیاز اجرا شود.

الزام B19: فروشنده باید راهنمایی امنیتی مستند کافی برای ادغام هر یک از اجزای امن را به یک پایانه POI ورود PIN ارائه دهد.

الزام B20: یک سیاست امنیتی دسترسی کاربر از فروشنده باید استفاده مناسب از POI در حالت امن، از جمله اطلاعات مسئولیت مدیریت کلید، مسئولیت مدیریتی، کارایی دستگاه، شناسایی، و الزامات محیطی را دارا باشد. سیاست امنیتی باید نقش پشتیبانی توسط POI را تعریف و خدمات در دسترس هر نقش را در قالب جدولی قطعی نشان دهد. POI قادر به انجام قابلیت‌های تعریف شده است، یعنی هیچ قابلیت پنهانی وجود ندارد.

الزام C: الزامات امنیتی PIN آنلاین

الزام C1: اگر دستگاه بتواند چند کلید رمزنگاری PIN نگه دارد و اگر کلید مورداستفاده برای رمزنگاری PIN بتواند از بیرون انتخاب شود، دستگاه باید جایگزینی کلیدهای غیرمجاز و سوء استفاده از کلید را ممنوع کند.

الزام D: الزامات امنیتی PIN آفلاین

الزام D1: امکان نفوذ ریدر ICC برای اعمال اضافات، تعویض، و یا تغییرات سخت-افزار و یا نرم‌افزار ریدر ICC ، به منظور تعیین و یا تغییر اطلاعات حساس، بدون نیاز به حداقل پتانسیل حمله ۲۰ برای شناسایی و بهره‌برداری اولیه، با حداقل ۱۰ برای بهره‌برداری وجود نداشته باشد. همچنین امکان اقامت کارت IC و هر جسم خارجی دیگر در داخل محل قرارگیری کارت وجود نداشته باشد.

نکته: تمامی حملات باید شامل حداقل زمان حمله ۱۰ ساعته برای بهره‌برداری باشد.

الزام D2: شروع قرارگیری کارت IC در طول قرارگیری کارت، جهت تشخیص موانع نامطلوب و یا مشکوک تحت نظر کامل دارنده کارت باشد.

الزام D3: ریدر ICC به طوری ساخته شده که سیم‌های بیرون از محل شکاف ریدر IC به یک دستگاه ضبط و یا یک فرستنده (یک bug خارجی) توسط دارنده کارت قالب مشاهده باشد.

الزام D4: برای حفاظت از PIN در زمان انتقال بین دستگاه رمزنگاری PIN و ریدر ICC حداقل باید دو مورد زیر در نظرگرفته شود:

- اگر دستگاه PIN را رمزنگاری نموده و ریدر ICC در داخل همان ماژول امن یکپارچه نشده باشد، روش تأیید صحت دارنده کارت به صورت زیر تعیین می‌شود:
  - یک PIN رمزشده: بلوک PIN باید بین دستگاه رمزنگاری PIN و ریدر ICC با استفاده از کلید رمزنگاری تصدیق‌شده کارت IC، و یا مطابق با ISO 9564 رمزنگاری شود.

- یک PIN متنی: بلوک PIN باید از دستگاه رمزنگاری PIN به ریدر ICC مطابق با استاندارد ISO 9564 رمزشود. (سپس ریدر ICC اقدام به رمزگشایی PIN و انتقال آن به صورت متنی به کارت IC می-نماید).

➢ اگر دستگاه PIN را رمزنگاری نموده و ریدر ICC در داخل همان ماژول امن یکپارچه شده باشد، روش تأیید صحت دارنده کارت به صورت زیر تعیین می‌شود:

- یک پین رمزشده: بلوک PIN باید با استفاده از یک کلید رمزنگاری تصدیق‌شده کارت IC رمزنگاری شود.
- یک PIN متنی: اگر بلوک PIN از یک محیط کاملا حفاظت‌شده منتقل شود رمزنگاری لازم نیست (طبق تعریف ISO 9564). اگر PIN متنی به ریدر ICC از طریق یک محیط محافظت نشده منتقل شود، بلوک PIN باید مطابق با استاندارد ISO 9564 رمزنگاری شود.

۲) ماژول ۲: یکپارچه‌سازی پایانه

الزام E: الزامات امنیتی یکپارچه‌سازی پایانه POS

مدیریت پیکربندی

الزام E1: هر یک از اجزای امن یکپارچه با ورودی PIN پایانه POI که برای ارزیابی ارائه می‌شود، یک محیط امنیتی فیزیکی و منطقی واضح دارد. (مربوط به ورودی PIN و قابلیت خواندن کارت)

یکپارچه‌سازی قابلیت ورودی PIN

الزام E2-1: ادغام منطقی و فیزیکی اجزا (یا قطعات) امن مورد تایید PCI با ورودی PIN پایانه POI نباید سطح حفاظت PIN کلی را تحت تاثیر قرار دهد.

الزام E2-2: پد PIN (منطقه ورود PIN) و مناطق اطراف آن باید در جهت ممانعت در برابر قرارگیری جعلی پوشش پد PIN طراحی و مهندسی شود.

یک حمله پوشش باید مستلزم حداقل پتانسیل حمله ۱۸ برای شناسایی و بهره‌برداری اولیه، با حداقل ۹ برای بهره‌برداری باشد.

یکپارچه‌سازی با پایانه فروش (POS)

الزام E3-1: ادغام منطقی و فیزیکی اجزای امن مورد تایید با ورودی PIN پایانه POI نباید مسیرهای حمله جدید به PIN ایجاد کند.

الزام E3-2: ورودی PIN پایانه POI با مکانیسم‌هایی برای جلوگیری از حملات با هدف حفظ و سرقت کارت پرداخت مجهز شود.

الزام E3-3: یک جداسازی منطقی و / یا فیزیکی واضح میان اجزای امن و اجزای غیر امن یکپارچه در یک دستگاه وجود دارد.

الزام E3-4: برنامه POI باید میان پیام‌های نمایش داده شده به دارنده کارت و حالت عملیاتی (مد امن یا غیرامن) دستگاه ورود PIN، با استفاده از احراز هویت رمزنگاری ارتباط ایجاد کند.

اگر دستورات به ارتباط میان پیام‌های نمایش داده شده به دارنده کارت و حالت عملیاتی دستگاه ورود PIN دریافتی از یک دستگاه خارجی (به عنوان مثال کنترل کننده فروش) تاثیر داشته باشد، بایستی ورود داده احراز هویت شود.

تغییر ارتباط میان پیام‌های نمایش داده شده به دارنده کارت و حالت عملیاتی دستگاه ورود PIN نمی‌تواند بدون نیاز به حداقل پتانسیل حمله ۱۸ به ازای هر POI برای شناسایی و بهره‌برداری اولیه، با حداقل ۱۰ برای بهره‌برداری رخ دهد.

الزام E3-5: پایانه POI پذیرش PIN باید تنها با یک رابط پذیرش PIN کارت پرداخت، به عنوان مثال، یک صفحه کلید مجهز شود. اگر رابط دیگری به عنوان یک صفحه کلید موجود باشد، مکانیسمی برای جلوگیری از استفاده از آن برای ورود PIN باید باشد. به

عنوان مثال، نباید کلیدهای عددی داشته باشد، و یا امکان استفاده از آن برای ورود اعداد را نداشته باشد، و یا مطابقت آن با B16 کنترل شود.

الزامات حذف

الزام E4-1: دستگاه در برابر حذف غیرمجاز محافظت شود. شکست یا دورزدن این مکانیزم باید نیاز به یک حداقل پتانسیل حمله ۱۸ به ازای هر دستگاه برای شناسایی و بهره-برداری اولیه، با حداقل ۹ برای بهره‌برداری داشته باشد.

الزام E4-2: اسناد فروشنده شامل جزئیات در مورد چگونگی پیاده‌سازی محافظت سیستم در برابر حذف غیرمجاز، حفظ و در دسترس یکپارچه‌سازان باشد.

الزام E4-3: برای هر دستگاه تعبیه‌شده، حفاظت از سیستم در برابر حذف غیرمجاز طبق اسناد سازنده آن باید اجرا شود.

۳) ماژول ۳: پروتکل‌های باز

الزام F: کشف

الزام F1: تمام پروتکل‌های دامنه‌ها و رابط‌های عمومی موجود بر روی دستگاه به وضوح در ماژول پروتکل باز و توسط فروشنده دستگاه تعریف شود - فرم اظهارنامه پروتکل. فروشنده یک درک کامل و جامع در مورد چگونگی تعامل تمام پروتکل‌ها و رابط‌های دستگاه حاضر دارد.

الزام G: ارزیابی آسیب‌پذیری

الزام G1: فروشنده دستگاه دارای سیاست‌ها و روش‌های داخلی جهت اطمینان از حفظ فرآیند موثر برای تشخیص آسیب‌پذیری دستگاه است. این فرآیند باید به اندازه کافی جهت پوشش تمام رابط‌های تعریف شده در F1 قوی باشد. این فرآیند باید به اندازه کافی برای تشخیص آسیب‌پذیری در ارزیابی موثر باشد.

الزام G2: دستگاه برای اطمینان از اینکه پروتکل‌ها و رابط‌های لیست شده در F1 شامل آسیب‌پذیری نباشد، باید تحت ارزیابی آسیب‌پذیری قرار گیرد.

- الف) ارزیابی آسیب‌پذیری از طریق آنالیز مستند توصیف شده برای امنیت پروتکل‌ها و رابط‌ها اجرا شود.
- ب) ارزیابی آسیب‌پذیری از طریق اطلاعات نظرسنجی عمومی آسیب‌پذیری اجرا شود.
- ج) ارزیابی آسیب‌پذیری از طریق تست اجرا شود.

الزام G3: فروشنده دستگاه دارای اقدامات افشای آسیب‌پذیری برای دستگاه است.

- الف) اقدامات افشای آسیب‌پذیری، مستند شود.
- ب) اقدامات افشای آسیب‌پذیری، توزیع به موقع اطلاعات در مورد آسیب-پذیری‌های تازه پیداشده را شامل شود. این اطلاعات شامل شناسایی، توصیف، و ارزیابی آسیب‌پذیری است.
- ج) اقدامات افشای آسیب‌پذیری، توزیع به موقع کاهش اقدامات را شامل شود.

الزام H: راهنمای فروشنده

الزام H1: دستگاه دارای راهنمای امنیتی جهت توضیح چگونگی استفاده از پروتکل‌ها و خدمات برای هر رابط است که در دسترس برنامه‌های کاربردی دستگاه می‌باشد.

الزام H2: دستگاه دارای راهنمایی جهت توصیف تنظیمات پیش‌فرض هر پروتکل و خدمات برای هر رابط است که در دسترس دستگاه می‌باشد. همه رابط و پروتکل‌های دستگاه باید دارای تنظیمات پیش‌فرض امن باشد. اگر رابط دارای قابلیت تنظیمات غیرامن باشد، راهنمای فروشنده باید نسبت به تنظیمات غیرامن هشدار دهد.

الزام H3: دستگاه دارای راهنمایی برای مدیریت کلید است که چگونگی استفاده کلید و گواهی‌نامه را توصیف می‌کند.

- الف) راهنمای مدیریت کلید در اختیار کاربران داخلی و / یا توسعه-دهندگان نرم‌افزار، یکپارچه‌سازان سیستم، و کاربران نهایی دستگاه باشد.

- ب) راهنمای امنیت مدیریت کلید ویژگی‌های همه کلیدها و گواهی‌نامه‌های قابل استفاده توسط دستگاه را توصیف می‌کند.
- ج) راهنمای امنیت مدیریت کلید مسئولیت‌های فروشنده دستگاه، توسعه-دهندگان نرم‌افزار، یکپارچه‌سازان سیستم، و کاربران نهایی دستگاه را توصیف می‌کند.
- د) راهنمای امنیت مدیریت کلید استفاده ایمن از کلید و گواهی‌نامه را تضمین می‌کند.

الزام I: تست عملیاتی

الزام I1: دستگاه دارای تمام پروتکل‌های امنیتی مشخص شده در ماژول پروتکل باز است - فرم اظهارنامه پروتکل. فروشنده دستگاه مدارک مربوط به توصیف پیاده‌سازی و استفاده از پروتکل‌های امنیتی دستگاه را تهیه می‌نماید.

الزام I2: دستگاه قادر به ارسال محرمانه اطلاعات بر روی اتصالات شبکه است.

- الف) مکانیزم رمزگذاری از اندازه کلید مناسب الگوریتم در پرسش‌ها استفاده می‌کند.
- ب) رمزگذاری با استفاده از کلیدهای ساخته شده به شیوه امن و با روش-های مدیریت کلید مناسب انجام می‌شود، مانند روش‌های مذکور در NIST SP 800-21، راهنمای پیاده‌سازی رمزنگاری در دولت فدرال و بانکداری ISO 11568.

الزام I3: دستگاه قادر به ارسال یکپارچه اطلاعات بر روی اتصالات شبکه است.

- الف) تمامیت و درستی توسط MAC معرفی شده در استاندارد ISO 16609، و یا با یک امضای دیجیتال انجام می‌شود.
- ب) هش با حداقل یکی از الگوریتم‌های SHA-224، SHA-256، SHA-384 و SHA-512 انجام می‌شود.

الزام I4: دستگاه از پروتکل امنیتی برای احراز هویت سرور استفاده می‌کند.

- الف) احراز هویت سرور از اندازه کلید مناسب الگوریتم پرسش مربوطه استفاده می‌کند.
- ب) هش با حداقل یکی از الگوریتم‌های SHA-224، SHA-256، SHA-384 و SHA-512 انجام می‌شود.
- ج) دستگاه قادر به بررسی اعتبار کلید عمومی دریافتی است.
- د) دستگاه قادر به بررسی صحت کلید عمومی دریافتی است.
- ه) گواهی‌نامه مورد اعتماد دستگاه باید تنها شامل گواهی کلید عمومی از CA مورد اعتماد و یا گواهی خود-امضا مورد تایید پذیرنده باشد.

الزام I5: دستگاه قادر به تشخیص پخش دوباره پیام و مدیریت امن استثناها است.

الزام I6: دستگاه مدیریت جلسه را اجرا می‌کند.

- الف) دستگاه مسیر همه اتصالات را حفظ و تعداد حداقل جلساتی که می‌تواند بر روی دستگاه فعال باشد را محدود می‌کند.
- ب) دستگاه محدودیت زمانی برای جلسات را تنظیم و باز نبودن جلسات بیش از مدت زمان موردنیاز را تضمین می‌کند.

الزام J: امنیت پیکربندی و نگهداری

الزام J1: فروشنده دستگاه راهنمای توصیف مدیریت پیکربندی دستگاه را ایجاد می‌کند.

- الف) راهنما در اختیار کاربران داخلی و / یا توسعه‌دهندگان نرم‌افزار، یکپارچه‌سازان سیستم، و کاربران نهایی دستگاه باشد.
- ب) راهنما کل دستگاه را پوشش دهد - از جمله سیستم عامل، برنامه‌های کاربردی پرداختی و غیرپرداختی، فرم‌ها، فایل‌های چندرسانه‌ای، گواهی‌نامه‌ها، فایل‌های پیکربندی، تنظیمات پیکربندی، و کلیدها.
- ج) راهنما چرخه کامل حیات دستگاه را از توسعه، تولید، تا تحویل و بهره‌برداری پوشش دهد.
- د) راهنمای امنیتی عدم امکان تغییر غیرمجاز را تضمین کند.

- ه) راهنمای امنیتی تضمین کند که هرگونه تغییر تاثیرگذار در امنیت دستگاه مورد تایید PTS، در نتیجه تغییر شناسه دستگاه است.

الزام J2: فروشنده دستگاه دارای اقدامات تعمیر و نگهداری است.

- الف) این اقدامات مستند شود.
- ب) این اقدامات در فعالیت‌های انجام شده در دوره‌های ارزیابی آسیب-پذیری شامل آنالیز، بررسی اطلاعات موجود در حوزه عمومی، و تست و آزمون تشخیص به موقع آسیب‌پذیری را تضمین نماید.
- ج) این اقدامات ارزیابی به موقع بوده و طبقه‌بندی آسیب‌پذیری‌های جدید پیداشده را تضمین کند.
- د) این اقدامات کاهش آسیب‌پذیری‌های جدید پیداشده و تاثیرگذار بر امنیت دستگاه را تضمین کند.

الزام J3: اگر یک دستگاه مستقر امکان آپدیت داشته باشد، فروشنده دستگاه راهنمای چگونگی آپدیت محلی و از راه دور را ایجاد کند.

الزام J4: مکانیسم آپدیت، امنیت را تضمین کند، به عنوان مثال، تمامیت و جامعیت، احراز هویت متقابل، و محافظت در برابر پخش دوباره، با استفاده از یک پروتکل امنیتی مناسب در زمان اتصال به شبکه. برای آپدیت‌های دستی، دسترسی مدیر باید با استفاده از رمز عبور / PIN و / یا تکنیک‌های احراز هویت رمزنگاری اجرا شود.

٤) ماژول ٤: خواندن و تبادل امن اطلاعات (SRED)

الزام K: حفاظت اطلاعات حساب

الزام K1: همه اطلاعات حساب یا بلافاصله پس از ورود رمزگذاری شده و یا به صورت متنی به یک دستگاه امن وارد شده و درون کنترلر امن دستگاه پردازش شود.

الزام K1-1: دستگاه تمام اطلاعات حساب را پس از ورود محافظت نماید (مطابق با A9 برای داده‌های نوار مغناطیسی و D1 برای داده‌های تراشه) ، و هیچ روش دسترسی به اطلاعات متنی حساب بدون شکست امنیتی دستگاه وجود ندارد (با استفاده از روش‌های

شرح داده شده در A1). شکست یا دور زدن مکانیزم امنیتی نیاز به حداقل پتانسیل حمله ۱۶ برای شناسایی و بهره‌برداری اولیه، با حداقل ۸ برای بهره‌برداری دارد.

نکته: MSR[1]ها و ICCR[2]ها باید به ترتیب پتانسیل حمله مندرج در DTRهای A9 و D1 را داشته باشند.

الزام K1-2: شکست یکی از مکانیزم‌های امنیتی تک، دلیل بر عدم تطبیق امنیت دستگاه نیست. حفاظت در مقابل یک تهدید بر اساس ترکیبی از حداقل دو مکانیزم امنیتی مستقل است.

الزام K2: ادغام منطقی و فیزیکی ریدر کارت امن مورد تایید با ورودی PIN پایانه POI مسیرهای حمله جدید به اطلاعات حساب ایجاد نکند. اطلاعات حساب در مسیر قسمت ورودی تا کنترلر امن دستگاه محافظت شود - یعنی امکان افشای اطلاعات حساس وجود ندارد.

الزام K3: تعیین هر کلید رمزنگاری مربوط به اطلاعات حساب موجود در این دستگاه، توسط نفوذ و / یا مانیتورینگ دستگاه (از جمله نوسانات برق)، به حداقل پتانسیل حمله ۲۶ برای شناسایی و بهره‌برداری اولیه با حداقل ۱۳ برای بهره‌برداری نیاز دارد.

الزام K3-1: کلیدهای عمومی باید به شیوه‌ای ذخیره و استفاده شوند که در برابر تغییرات غیرمجاز محافظت گردند. تغییرات غیرمجاز نیاز به حداقل پتانسیل حمله ۲۶ برای شناسایی و بهره‌برداری اولیه، با حداقل ۱۳ برای بهره‌برداری دارد.

الزام K4: همه اطلاعات حساب فقط باید با ANSI X9 یا الگوریتم‌های رمزنگاری مورد تایید ISO (به عنوان مثال، AES، TDES) رمزگذاری شوند.

الزام K5: اگر توزیع کلید از راه دور باشد، دستگاه از احراز هویت متقابل میان میزبان ارسال‌کننده توزیع کلید و دستگاه دریافت‌کننده پشتیبانی نماید.

---

[1] Magnetic Stripe Reader
[2] Integrated Circuit Card Reader

الزام K6: دستگاه از احراز هویت مبدا اطلاعات پیام‌های رمزگذاری‌شده پشتیبانی نماید.

الزام K7: کلیدهای خصوصی و محرمانه که در داخل دستگاه و برای پشتیبانی از رمزگذاری اطلاعات حساب می‌باشند به ازای هر دستگاه منحصر به فرد باشد.

الزام K8: رمزگذاری و یا رمزگشایی اطلاعات با استفاده از کلید رمزنگاری اطلاعات حساب یا کلید رمزنگاری کلید موجود در دستگاه مجاز نیست.

مقادیر کلید اطلاعات حساب، کلید رمزنگاری کلید، و کلید رمزنگاری PIN باید متفاوت باشند.

الزام K9: تمام دسترسی‌های مدیریتی از راه دور موجود در دستگاه باید به صورت رمزگذاری‌شده احراز هویت شود. اگر صحت درخواست دسترسی تایید نشود، درخواست دسترسی باید رد شود.

الزام K10: سیستم عامل و هرگونه تغییرات بعدی مطابق با B3 بازرسی و بررسی شود.

الزام K11-1: سیستم عامل باید صحت تمام برنامه‌های کاربردی بارگذاری شده بر روی پایانه را مطابق با B4 تایید کند. اگر دستگاه امکان آپدیت برنامه کاربردی و یا تنظیمات نرم-افزار را داشته باشد بایستی به صورت رمزنگاری شده آن را مطابق با B4 احراز هویت نماید.

الزام K11-2: فروشنده باید راهنمای امنیتی مطابق با B2 و B6 را به تمام توسعه-دهندگان برنامه کاربردی جهت تضمین موارد ذیل ارائه نماید:

- برنامه‌های کاربردی نباید توسط ناهنجاری‌های منطقی که بتواند باعث پاک شدن اطلاعات متنی خروجی در حالت رمزی پایانه باشد، تحت تاثیر قرار گیرد.
- اطلاعات حساب نباید به مدت طولانی حفظ و یا بیشتر از حد لازم استفاده شود.

الزام K12: اگر دستگاه امکان آپدیت سیستم عامل را داشته باشد بایستی به صورت رمزنگاری شده آن را احراز هویت نموده و در صورت عدم تایید رد و حذف شود.

الزام K13: قابلیت دستگاه نباید توسط ناهنجاری‌های منطقی مطابق با B2 تحت تاثیر قرار گیرد.

الزام K14: اگر دستگاه قادر به برقراری ارتباط بیش از یک شبکه IP و یا استفاده از یک پروتکل دامین عمومی (مانند Wi-Fi و یا بلوتوث) است، باید الزامات مشخص شده در ماژول DTR ۳ (پروتکل‌های باز) را برآورده سازد.

الزام K15: هنگامی که عملیات در حالت رمزگذاری است، مکانیزمی برای خروج اطلاعات حساب به صورت متنی در دستگاه وجود ندارد. تغییر میان حالت رمزنگاری و غیر رمزنگاری عملیات نیاز به احراز هویت صریح دارد.

الزام K15-1: هنگامی که عملیات در حالت رمزگذاری است، کنترلر امن می‌تواند اطلاعات حساب متنی را فقط در برنامه تصدیق شده منتشر کند.

الزام K15-2: اطلاعات حساب (در حالت متنی و یا به صورت رمزشده) نباید به مدت طولانی حفظ و یا بیشتر از حد لازم استفاده شود.

الزام K16: اگر دستگاه قادر به تولید مقادیر PAN جایگزین برای خروجی دستگاه باشد، تعیین PAN اصلی فقط با دانستن مقدار جایگزین نباید امکان‌پذیر باشد.

الزام K16-1: در صورت تولید مقادیر PAN جایگزین با استفاده از تابع هش، ورودی تابع باید از یک Salt[1] با حداقل طول ۶۴ بیت استفاده کند.

الزام K16-2: در صورت تولید مقادیر PAN جایگزین با استفاده از تابع هش، Salt باید محرمانه مانده و به صورت مناسب محافظت شود. افشای Salt نمی‌تواند بدون نیاز به یک حداقل پتانسیل حمله ۱۶ به ازای هر دستگاه برای شناسایی و بهره‌برداری اولیه با حداقل ۸ برای بهره‌برداری رخ دهد.

الزام K17: تکنیک‌های مدیریت کلید، مطابق با B11 در دستگاه اجرا شود.

---

[1] داده تصادفی است که به عنوان یک ورودی اضافی در یک تابع یک طرفه هش استفاده می‌شود.

الزام K18: دستگاه دارای ویژگی پیشگیری و یا جلوگیری قابل توجهی در استفاده از دستگاه برای تعیین کامل PAN باشد.

الزام K19: تغییر شرایط محیطی و یا عملیاتی (مثلا دما یا ولتاژ خارج از محدوده عملیاتی) نباید بر روی تطابق امنیتی دستگاه، و یا خروج اطلاعات حساب به صورت متنی از دستگاه تاثیر گذارد.

الزام K20: اگر دستگاه از نرم‌افزارهای متعدد پشتیبانی کند، باید آنها را مطابق با B17 تفکیک کند.

الزام K21: سیستم عامل دستگاه باید ویژگی‌های زیر را داشته باشد:

- سیستم عامل دستگاه باید تنها شامل نرم‌افزار (اجزاء و خدمات) لازم برای عملکرد در نظر گرفته شده باشد.
- سیستم عامل باید به صورت امن پیکربندی و با حداقل امتیاز اجرا شود.
- سیاست امنیتی نباید اجازه اجرای قابلیت‌های غیرمجاز و یا غیرضروری را بدهد.
- قابلیت و دستورات APIای که موردنیاز قابلیت‌های خاص نباشند باید غیرفعال (و در صورت امکان، حذف) شوند.

الزام K22: دسترسی به سرویس‌های حساس نیاز به احراز هویت داشته باشد. سرویس-های حساس زمینه دسترسی به قابلیت‌های حساس را فراهم می کند. قابلیت‌های حساس همان پردازش داده‌های حساس مانند کلیدهای رمزنگاری، اطلاعات حساب، و کلمه عبور می‌باشد. ورود یا خروج سرویس‌های حساس نباید آشکار شده و یا بر داده‌های حساس تاثیر گذارد.

الزام K23: سرویس‌های حساس در برابر استفاده غیرمجاز مطابق با B8 محافظت شود.

۵) ماژول ۵: الزامات امنیتی مدیریت دستگاه

الزام L: در طول ساخت

الزام L1: روش‌های کنترل تغییر قابلیت‌های فیزیکی و یا عملکردی POI باید تحت الزامات امنیتی فیزیکی و یا منطقی مجدداً بررسی و تصدیق شود. بررسی تغییراتی که صرفا جهت اصلاح خطاها و گسل‌ها در نرم‌افزار در راستای قابلیت در نظر گرفته شده بوده و عمل حذف، ویرایش، و یا افزایش قابلیت انجام ندهد، نیازی به بررسی مجدد ندارد. تصویب پذیرش Delta مشروط به مدارک فرآیند کنترل تغییر و مدیریت آسیب‌پذیری در حال انجام باشد.

الزام L2: سیستم عامل تاییدشده در جهت جلوگیری از تغییر غیرمجاز در طول کل چرخه ساخت محافظت و ذخیره می‌شود. به عنوان مثال با استفاده از کنترل دوگانه و یا روش‌های احراز هویت رمزنگاری استاندارد.

الزام L3: قطعات مورد استفاده در مونتاژ دستگاه توسط ارزیابی الزامات اصلی امنیتی یکپارچه پایانه POS و یا ورودی PIN تایید شده و تغییرات غیرمجاز اعمال نشود.

الزام L4: جهت جلوگیری از تغییرات غیرمجاز نرم‌افزار تولیدی (به عنوان مثال، سیستم عامل) که در زمان ساخت دستگاه بارگذاری می‌شود، باید تحت اصول کنترل دوگانه انتقال، ذخیره ، و استفاده شود.

الزام L5: دستگاه و هر یک از اجزای آن بعد از تولید اما قبل از انتقال از سازنده به مرکز فروش، در یک منطقه محافظت‌شده و کنترل‌شده از نظر دسترسی و یا در بسته‌بندی Tamper آشکار برای جلوگیری از دسترسی‌های غیرمجاز کشف‌نشده به دستگاه و یا اجزای آن نگهداری شود.

الزام L6: اگر دستگاه در مرکز بارگذاری کلید و یا مرکز استقرار اولیه با استفاده از اطلاعات محرمانه قرار داده شده در دستگاه در طول تولید، احراز هویت شود، بایستی این اطلاعات محرمانه برای هر دستگاه منحصر به فرد و برای هر شخص ناشناخته و غیرقابل پیش‌بینی بوده، و برای جلوگیری از افشای در طول نصب، تحت کنترل دوگانه نصب شود.

الزام L7: اقدامات امنیتی در طول توسعه و نگهداری اجزای مربوط به امنیت POI بایستی اعمال شود. سازنده باید مستندات امنیتی توسعه شامل توصیف تمام اقدامات فیزیکی، رویه‌ای، پرسنل، و سایر اقدامات امنیتی موردنیاز حفاظت از یکپارچگی طراحی و پیاده‌سازی اجزای مربوط به امنیت POI در محیط توسعه خود را ایجاد کند. اسناد و مدارک امنیتی توسعه باید نشان دهد که این اقدامات امنیتی در راستای توسعه و نگهداری اجزای مربوط به امنیت POI بوده و سطح موردنیاز حفاظت برای حفظ یکپارچگی اجزای مربوط به امنیت POI را فراهم می‌کند.

الزام L8: فرآیند پردازش، کنترل می‌گردد، از جمله تنظیم مجدد مکانیزم Tamper، و فرآیند بازرسی / تست پس از تعمیر جهت تضمین عدم تغییر غیرمجاز دستگاه.

الزام M: بین ساخت و مرکز بارگذاری کلید اولیه و یا مرکز استقرار اولیه

الزام M1: POI باید در برابر تغییرات غیرمجاز با ویژگی‌های امنیتی Tamper آشکار محافظت شود، و مستندات آموزش اعتبارسنجی صحت و یکپارچگی POI (هم محصولات انتقال یافته و هم قابل دسترس ایمن آنلاین) باید در دسترس مشتریان باشد.

در صورت عدم امکان مورد مذکور، POI از مرکز ساخت به مرکز بارگذاری کلید اولیه یا مرکز استقرار اولیه منتقل و نگهداری شده و در مسیر خود تحت کنترل ممیزی برای آگاهی از محل POI در هر زمان می‌باشد.

در صورت تعدد شرکا برای انتقال، تضمین مدیریت انتقال و نگهداری در راستای مطابقت با الزامات به عهده هر یک از آنها خواهد بود.

الزام M2: مسئولیت روش‌های انتقال دستگاه از مرکز ساخت به مرکز استقرار اولیه در محل می‌باشد. در صورت انتقال از طریق واسطه‌ها، مانند نمایندگان فروش، از زمان دریافت دستگاه تا زمان تحویل به واسطه بعدی یا محل استقرار اولیه مسئولیت آن با همان واسطه خواهد بود.

الزام M3: در زمان انتقال دستگاه از مرکز ساخت به مرکز بارگذاری کلید اولیه، دستگاه باید:

- در بسته‌بندی Tamper آشکار حمل و ذخیره شود؛ و / یا
- به صورت محرمانه حمل و ذخیره شده به طوری که در صورت تلاش تغییر فیزیکی یا عملکردی بلافاصله و به طور خودکار پاک شده، و توسط مرکز بارگذاری کلید اولیه بتواند بازبینی شود، اما توسط افراد غیرمجاز تعیین نشود.

الزام M4: امنیت توسعه دستگاه برای مرکز بارگذاری کلید اولیه جهت تضمین صحت اجزاء مربوط به امنیت TOE[1] (هدف ارزیابی) بایستی مستندسازی شود.

الزام M5: اگر سازنده مسئول بارگذاری کلید اولیه باشد، باید صحت قطعات مربوط به امنیت POI را بررسی و تایید کند.

الزام M6: اگر سازنده مسئول بارگذاری کلید اولیه نباشد، باید وسیله‌ای برای مرکز بارگذاری کلید اولیه جهت تضمین صحت اجزاء مربوط به امنیت POI فراهم کند.

الزام M7: هر دستگاه باید یک شناسه منحصر به فرد قابل مشاهده و چسبیده به آن داشته باشد.

الزام M8: فروشنده باید یک راهنمای کاربر شامل دستورالعمل مدیریت عملیاتی POI فراهم نماید، که شامل دستورالعمل ثبت چرخه کل حیات اجزاء مربوط به امنیت POI و شیوه یکپارچه‌سازی این اجزا در یک دستگاه POI است. به عنوان مثال:

- اطلاعات تولید و شخصی‌سازی
- حدود زمانی / فیزیکی
- تعمیر و نگهداری
- عزل عملیات
- مفقودی یا سرقتی

[1] Target Of Evaluation

قابلیت‌های پشتیبانی شده توسط دستگاه POI و الزامات مربوطه

۱) قابلیت‌های دستگاه POI

قابلیت‌های یک دستگاه POI به هشت قسمت تقسیم می‌شود:

- **ورودی PIN:** قابلیت گرفتن PIN از دارنده کارت و تبدیل آن به اطلاعات است.
- **کلیدها:** این قابلیت مربوط به کلیدهای درگیر با امنیت PIN است. این کلیدها شامل کلید الگوریتم متقارن، کلید خصوصی الگوریتم نامتقارن، و کلید عمومی الگوریتم نامتقارن (با محدودیت صحت و تمامیت) می‌باشد.
- **ریدر کارت:** قابلیت گرفتن اطلاعات کارت، صرف نظر از تکنولوژی استفاده شده (به عنوان مثال، هم ریدر نوار مغناطیسی و هم ریدر کارت هوشمند). این قابلیت به دو بخش ICCR و MSR تقسیم می‌شود.
- **بازخورد به دارنده کارت:** بازخورد می‌تواند به صورت شنوایی و قابل مشاهده (به عنوان مثال، صفحه نمایش) و ... باشد.
- **پایانه یک ماژول است:** یعنی دستگاه تحت ارزیابی به صورت تجهیزات یکپارچه طراحی شده است. ماژول به تجهیزات OEM[1] اشاره دارد.
- **پایانه یک جسم ترکیبی است:** دستگاه تحت ارزیابی، به دلیل دربرداشتن چندین ماژول به منظور پوشش قابلیت‌های مذکور ترکیبی است. ترکیبی بودن دستگاه با قابلیت "پایانه یک ماژول است" تداخلی ندارد. هر دو قابلیت مستقل هستند.
- **پایانه پشته TCP/IP را پیاده‌سازی می‌کند:** دستگاه تحت ارزیابی، پشته TCP / IP و پروتکل‌های باز مرتبط را پیاده‌سازی می‌کند.
- **حفاظت از اطلاعات حساب:** امن نمودن اطلاعات حساب مطابق با ماژول خواندن و تبادل امن اطلاعات (SRED).

[1] Original Equipment Manufacturer

۲) رابطه الزامات با قابلیت‌های دستگاه POI

جدول ٤-٤: رابطه الزامات با قابلیت‌های دستگاه POI

الزام	ورودی PIN	کلیدها	ICCR	MSR	بازخورد به دارنده کارت	پایانه یک ماژول است	پایانه یک جسم ترکیبی است	پیاده‌سازی پشته TCP/IP	حفاظت از اطلاعات حساب	شرایط
ماژول الزامات اصلی										
الزامات امنیتی اصلی فیزیکی										
A1	×									
A2	×	×								
A3	×	×								
A4	×	×								
A5	×									
A6		×								
A7					×					
A8	×									در صورت امکان استفاده از صفحه کلید برای ورود داده غیر PIN
A9				×						
A10			×			×				
A11	×				×					
الزامات امنیتی اصلی منطقی										
B1	×	×						×	×	
B2	×	×								

الزام	ورودی PIN	کلیدها	ICCR	MSR	بازخورد به دارنده کارت	پایانه یک ماژول است	پایانه یک جسم ترکیبی است	پیاده‌سازی پشته TCP/IP	حفاظت از اطلاعات حساب	شرایط
B3	×	×								
B4	×	×								
B4-1	×	×								
B4-2	×	×							×	
B5	×									
B6	×									
B7	×	×								
B8	×	×								
B9		×						×	×	
B10	×									
B11		×								
B12	×	×								
B13	×	×			×					
B14	×	×								
B15	×									
B16					×					در صورت امکان استفاده از صفحه کلید برای ورود داده غیر PIN
B17	×									
B18	×									
B19			×	×		×				

الزام	ورودی PIN	کلیدها	ICCR	MSR	بازخورد به دارنده کارت	پایانه یک ماژول است	پایانه یک جسم ترکیبی است	پیاده‌سازی پشته TCP/IP	حفاظت از اطلاعات حساب	شرایط
B120	×	×	×	×	×	×	×	×	×	
الزامات امنیتی PIN آنلاین										
C1		×								
الزامات امنیتی PIN آفلاین										
D1 الی D4			×							
ماژول یکپارچه‌سازی پایانه										
الزامات امنیتی یکپارچه‌سازی پایانه POS										
E1	×	×	×		×	×	×	×	×	همیشه قابل اجرا است.
E2-1	×						×			
E2-2	×						×			
E3-1							×			
E3-2			×			×	×			
E3-3	×						×			
E3-4	×				×		×			در صورت امکان استفاده از صفحه کلید برای ورود داده غیر PIN
E3-5	×						×			
E4-1	×		×			×				
E4-2	×		×			×				
E4-3							×			

الزام	ورودی PIN	کلیدها	ICCR	MSR	بازخورد به دارنده کارت	پایانه یک ماژول است	پایانه یک جسم ترکیبی است	پیاده‌سازی پشته TCP/IP	حفاظت از اطلاعات حساب	شرایط
ماژول امنیت پروتکل‌های باز										
F الی I								×		همه الزامات
الزامات امنیت پیکربندی و نگهداری										
J1 الی J4	×	×	×	×	×	×	×	×	×	همه الزامات
ماژول خواندن و تبادل امن اطلاعات (SRED)										
K1 الی K23									×	همه الزامات
ماژول الزامات امنیتی دستگاه										
در طول ساخت										
L1 الی L8	×	×	×	×	×	×	×	×	×	
بین ساخت و مرکز بارگذاری کلید اولیه										
M1 الی M4	×	×	×	×	×	×	×		×	

الزامات استاندارد PCI PTS HSM

HSMها می‌توانند از انواع برنامه‌های کاربردی و فرآیندهای پردازش پرداخت و احرازهویت دارنده کارت پشتیبانی کنند که الزامات آن مربوط به موارد زیر می‌باشد:

- پردازش PIN
- امنیت 3D

- تایید کارت
- تولید و شخصی‌سازی کارت
- EFT POS
- تبادل ATM
- بارگذاری مجدد کارت نقد
- یکپارچگی داده
- پردازش تراکنش کارت تراشه

الزامات امنیتی این استاندارد در ماژول‌های امنیتی سخت‌افزار (PCI PTS HSM) به ۵ گروه به شرح جدول ذیل تقسیم می‌شود:

جدول ۴-۵: الزامات امنیتی PCI PTS HSM

الزامات
الزامات امنیتی فیزیکی
الزامات امنیتی منطقی
سیاست و روش‌ها
الزامات امنیتی دستگاه در طول ساخت
الزامات امنیتی دستگاه بین ساخت و مرکز استقرار اولیه

۱) A: الزامات امنیتی فیزیکی

الزام HSM :A1 از مکانیسم‌های تشخیص و پاسخ Tamper استفاده می‌کند که باعث از کار افتادن بلافاصله آن و در نتیجه پاک شدن اتوماتیک و فوری اطلاعات حساس ذخیره شده در دستگاه می‌شود، به طوری که غیرقابل بازیابی می‌گردد. این مکانیسم HSM را در برابر نفوذ فیزیکی محافظت می‌نماید، و به هیچ وجه قابلیت غیرفعال نمودن و یا شکست نداشته و یا دسترسی به اطلاعات حساس حوزه داخلی بدون نیاز به حداقل پتانسیل حمله ۲۶ به ازای هر دستگاه برای شناسایی و بهره‌برداری اولیه، با حداقل ۱۳ برای بهره‌برداری، وجود ندارد.

الزام A2: شکست یکی از مکانیزم‌های امنیتی تک، دلیل عدم تطبیق امنیت HSM نیست. حفاظت در مقابل یک تهدید بر اساس ترکیبی از حداقل دو مکانیزم امنیتی مستقل است.

الزام A3: در صورت وجود دسترسی به مناطق داخلی (به عنوان مثال، برای خدمات یا تعمیر و نگهداری)، امکان دسترسی به اطلاعات حساس آن منطقه وجود نداشته باشد. از دسترسی فوری به اطلاعات حساس، مانند PIN و یا داده‌های رمزنگاری، با طراحی درست مناطق داخلی و / یا بکارگیری مکانیسم پاک شدن فوری اطلاعات حساس، جلوگیری شود.

الزام A4: امنیت HSM با تغییر شرایط محیطی و شرایط عملیاتی در معرض خطر نباشد. (مثلاً تغییرات دما یا ولتاژ)

الزام A5: توابع و یا داده‌های حساس فقط در مناطق حفاظت شده این دستگاه استفاده می‌شوند. اطلاعات و توابع حساس یعنی داده‌های حساسی که در برابر تغییرات، بدون نیاز به حداقل پتانسیل حمله ۲۶ به ازای هر HSM برای شناسایی و بهره‌برداری اولیه، حداقل ۱۳ برای بهره‌برداری، محافظت شده است.

الزام A6: هیچ راه عملی برای تعیین اطلاعات حساس توسط انتشار الکترومغناطیسی مانیتورینگ، مصرف برق و یا سایر ویژگی‌های درونی و بیرونی بدون نیاز به حداقل پتانسیل حمله ۲۶ برای شناسایی و بهره‌برداری اولیه با حداقل ۱۳ برای بهره‌برداری وجود ندارد.

الزام A7: تعیین هر کلید رمزنگاری مربوط به PCI موجود در این دستگاه، توسط نفوذ و / یا مانیتورینگ دستگاه (از جمله نوسانات برق)، به حداقل پتانسیل حمله ۳۵ برای شناسایی و بهره‌برداری اولیه با حداقل ۱۵ برای بهره‌برداری نیاز دارد.

۲) B: الزامات امنیتی منطقی

الزام B1: دستگاه یک خود-آزمون، برای اطمینان از عملکرد منطبق بر طراحی پس از راه‌اندازی انجام داده و حداقل یک بار در روز صحت سیستم عامل و حالت خطر و Tampering را بررسی نماید. در صورت انجام عملیات مهم خاص، آزمون شرطی انجام دهد.

الزام B2: قابلیت HSM نباید توسط ناهنجاری‌های منطقی از جمله توالی دستور غیرمنتظره، دستورات ناشناخته، دستوراتی در حالت نادرست دستگاه و تامین پارامتر و یا داده‌های نادرست که بتواند باعث ایجاد خروجی متن واضح PIN و یا سایر داده‌های حساس در HSM شود، تحت تاثیر قرار گیرد.

الزام B3: سیستم عامل و هرگونه تغییرات بعدی بازرسی و با استفاده از فرایند ممیزی و مستند بررسی شده و در برابر قابلیت‌های پنهان وغیرمجاز و یا غیرمستند تضمین شود.

الزام B4: اگر HSM امکان آپدیت سیستم عامل را داشته باشد بایستی به صورت رمزنگاری شده آن را احراز هویت نموده و در صورت عدم تایید رد و حذف شود.

الزام B5: HSM واسط‌های امنی فراهم می کند که از طریق تمایز میان داده‌ها و کنترل ورودی‌ها و همچنین میان داده‌ها و وضعیت خروجی به صورت منطقی و جداگانه نگهداری می‌شوند.

الزام B6: HSM باید به طور خودکار بافر داخلی خود را برای جلوگیری از استفاده مجدد از اطلاعات حساس درون بافر، در زمان‌های اتمام تراکنش، اتمام زمان انتظار پاسخ و در حالت بروز خطا پاک کند.

الزام B7: دسترسی به سرویس‌های حساس نیاز به احراز هویت داشته باشد. سرویس-های حساس زمینه دسترسی به قابلیت‌های حساس را فراهم می کند. قابلیت‌های حساس همان پردازش داده‌های حساس مانند کلیدهای رمزنگاری، PIN، و کلمه عبور می‌باشد. ورود یا خروج سرویس‌های حساس نباید آشکار شده و یا بر داده‌های حساس تاثیر گذارد.

الزام B8: ورود کلید خصوصی و محرمانه با استفاده از تکنیک پذیرفته شده مطابق با جدول زیر انجام می‌شود.

جدول ۴-۶: تکنیک ورود انواع کلیدها

فرم کلید	تکنیک		
	دستی	مستقیم	شبکه
کلید متنی	خیر	بله	خیر
اجزای کلید متنی	بله	بله	خیر
کلید رمزنگاری شده	بله	بله	بله

الزام B9: اگر اعداد تصادفی مرتبط با امنیت اطلاعات حساس توسط دستگاه تولید شود، مولد عدد تصادفی جهت اطمینان از غیرقابل پیش‌بینی بودن اعداد بایستی ارزیابی شود.

الزام B10: HSM از الگوریتم‌ها، روش‌ها و اندازه کلیدهای رمزنگاری مورد قبول استفاده می‌کند.

الزام B11: تکنیک‌های مدیریت کلید، مطابق با ISO 11568 و / یا ANSI X9.24 پیاده‌سازی شود. تکنیک‌های مدیریت کلید، باید از روش استخراج کلید ANSI TR-31 و یا یک روش معادل برای حفظ باندل کلید TDEA پشتیبانی کند.

الزام B12: اگر کلیدهای رمزنگاری در محدوده امن HSM به هر دلیلی (Tamper یا عدم اعمال نیرو به مدت طولانی) اشتباه ارائه گردد، HSM به شیوه‌ای امن رد خواهد شد.

الزام B13: هر کلید رمزگذاری تنها برای یک قابلیت رمزنگاری استفاده شود. رمزگذاری یا رمزگشایی هر داده دلخواه با استفاده از کلید رمزنگاری PIN و یا کلید رمزنگاری کلید امکان‌پذیر نباشد.

الزام B14: هیچ مکانیزمی جهت خروج متن خصوصی و یا PIN، افشای رمزنگاری یک کلید یا PIN تحت یک کلید و یا انتقال متن واضح کلید از یک قسمت با امنیت بالا به یک قسمت با امنیت پایین‌تر در دستگاه وجود ندارد.

الزام B15: HSM برای مدیریت PIN طراحی شده است، تکنیک رمزگذاری PIN براساس تکنیک موجود در ISO 9564 اجرا شود.

الزام B16: HSM شامل مکانیسم‌های رمزنگاری برای پشتیبانی ورود امن به تراکنش-ها، داده‌ها، و رویدادها است.

الزام B17: اگر HSM از نرم‌افزارهای متعدد پشتیبانی می‌کند، باید آنها را تفکیک کند. نباید امکان تداخل و یا دستکاری با برنامه دیگر و یا سیستم عامل را داشته باشد، مثلا تغییر موضوع داده‌های متعلق به برنامه دیگر و یا سیستم عامل. به طور مشابه، در صورت پشتیبانی از مجازی‌سازی، باید به عنوان چند HSM جداگانه منطقی استفاده شود.

الزام B18: سیستم عامل این دستگاه باید شامل نرم‌افزار (قطعات و خدمات) لازم برای عملکرد مدنظر باشد. سیستم عامل باید به صورت امن پیکربندی و با حداقل امتیاز اجرا شود.

الزام B19: HSM باید یک ID منحصر به فرد داشته باشد.

الزام B20: HSMهای طراحی شده برای هر دو حالت PCI و غیر PCI نباید از کلیدهای محرمانه و یا خصوصی مشترک در هر دو حالت استفاده کند، باید مشخصه‌ای برای هر دو حالت داشته و احراز هویت دوگانه در زمان سوئیچ میان دو حالت انجام دهد.

۳) C: سیاست و روش‌ها

الزام C1: یک سیاست امنیتی دسترسی کاربر از فروشنده باید استفاده مناسب از HSM در حالت امن، از جمله اطلاعات مسئولیت مدیریت کلید، مسئولیت مدیریتی، کارایی دستگاه، شناسایی، و الزامات محیطی را دارا باشد. سیاست امنیتی باید نقش پشتیبانی توسط HSM را تعریف و خدمات در دسترس هر نقش را در قالب جدولی قطعی نشان دهد. HSM قادر به انجام قابلیت‌های تعریف شده است، یعنی هیچ قابلیت پنهانی وجود ندارد.

٤) D: الزامات امنیتی دستگاه در طول ساخت

الزام D1: روش‌های کنترل تغییر قابلیت‌های فیزیکی و یا عملکردی HSM باید تحت الزامات امنیتی فیزیکی و یا منطقی مجدداً بررسی و تصدیق شود. بررسی تغییراتی که صرفا جهت اصلاح خطاها و گسل‌ها در نرم‌افزار در راستای قابلیت در نظر گرفته شده بوده و عمل حذف، ویرایش، و یا افزایش قابلیت انجام ندهد، نیازی به بررسی مجدد ندارد.

الزام D2: سیستم عامل تاییدشده در جهت جلوگیری از تغییر غیرمجاز در طول کل چرخه ساخت محافظت و ذخیره می‌شود. به عنوان مثال با استفاده از کنترل دوگانه و یا روش‌های احراز هویت رمزنگاری استاندارد.

الزام D3: قطعات مورد استفاده در مونتاژ دستگاه توسط ارزیابی الزامات اصلی امنیتی تایید شده و تغییرات غیرمجاز اعمال نشود.

الزام D4: جهت جلوگیری از تغییرات غیرمجاز نرم‌افزار تولیدی (به عنوان مثال، سیستم عامل) که در زمان ساخت دستگاه بارگذاری می‌شود، باید تحت اصول کنترل دوگانه انتقال، ذخیره ، و استفاده شود.

الزام D5: HSM و هر یک از اجزای آن بعد از تولید اما قبل از انتقال از سازنده به مرکز فروش، در یک منطقه محافظت‌شده و کنترل‌شده از نظر دسترسی و یا در بسته‌بندی Tamper آشکار برای جلوگیری از دسترسی‌های غیرمجاز کشف‌نشده به دستگاه و یا اجزای آن نگهداری شود.

الزام D6: اگر HSM در مرکز بارگذاری کلید و یا مرکز استقرار اولیه با استفاده از اطلاعات محرمانه قرار داده شده در دستگاه در طول تولید، احراز هویت شود، بایستی این اطلاعات محرمانه برای هر HSM منحصر به فرد و برای هر شخص ناشناخته و غیرقابل پیش‌بینی بوده، و برای جلوگیری از افشای در طول نصب، تحت کنترل دوگانه نصب شود.

الزام D7: اقدامات امنیتی در طول توسعه و نگهداری اجزای مربوط به امنیت HSM بایستی اعمال شود. سازنده باید مستندات امنیتی توسعه شامل توصیف تمام اقدامات فیزیکی، رویه‌ای، پرسنل، و سایر اقدامات امنیتی موردنیاز حفاظت از یکپارچگی طراحی و

پیاده‌سازی اجزای مربوط به امنیت HSM در محیط توسعه خود را ایجاد کند. اسناد و مدارک امنیتی توسعه باید نشان دهد که این اقدامات امنیتی در راستای توسعه و نگهداری اجزای مربوط به امنیت HSM بوده و سطح موردنیاز حفاظت برای حفظ یکپارچگی اجزای مربوط به امنیت HSM را فراهم می‌کند.

الزام D8: فرآیند پردازش، کنترل می‌گردد، از جمله تنظیم مجدد مکانیزم Tamper، و فرآیند بازرسی/ تست پس از تعمیر جهت تضمین عدم تغییر غیرمجاز دستگاه.

۵) E: الزامات امنیتی دستگاه بین ساخت و مرکز استقرار اولیه

الزام E1: HSM باید در برابر تغییرات غیرمجاز با ویژگی‌های امنیتی Tamper آشکار محافظت شود، و مستندات آموزش اعتبارسنجی صحت و یکپارچگی HSM (هم محصولات انتقال یافته و هم قابل دسترس ایمن آنلاین) باید در دسترس مشتریان باشد.

در صورت عدم امکان مورد مذکور، HSM از مرکز ساخت به مرکز بارگذاری کلید اولیه یا مرکز استقرار اولیه منتقل و نگهداری شده و در مسیر خود تحت کنترل ممیزی برای آگاهی از محل HSM در هر زمان می‌باشد.

در صورت تعدد شرکا برای انتقال، تضمین مدیریت انتقال و نگهداری در راستای مطابقت با الزامات به عهده هر یک از آنها خواهد بود.

الزام E2: مسئولیت روش‌های انتقال دستگاه از مرکز ساخت به مرکز استقرار اولیه در محل می‌باشد. در صورت انتقال از طریق واسطه‌ها، مانند نمایندگان فروش، از زمان دریافت دستگاه تا زمان تحویل به واسطه بعدی یا محل استقرار اولیه مسئولیت آن با همان واسطه خواهد بود.

الزام E3: در زمان انتقال دستگاه از مرکز ساخت به مرکز بارگذاری کلید اولیه، دستگاه باید:

- در بسته‌بندی Tamper آشکار حمل و ذخیره شود؛ و / یا

- به صورت محرمانه حمل و ذخیره شده به طوری که در صورت تلاش تغییر فیزیکی یا عملکردی بلافاصله و به طور خودکار پاک شده، و توسط مرکز بارگذاری کلید اولیه بتواند بازبینی شود، اما توسط افراد غیرمجاز تعیین نشود.

الزام E4: امنیت توسعه دستگاه برای مرکز بارگذاری کلید اولیه جهت تضمین صحت اجزاء مربوط به امنیت TOE (هدف ارزیابی) بایستی مستندسازی شود.

الزام E5: اگر سازنده مسئول بارگذاری کلید اولیه باشد، باید صحت قطعات مربوط به امنیت HSM را بررسی و تایید کند.

الزام E6: اگر سازنده مسئول بارگذاری کلید اولیه نباشد، باید وسیله‌ای برای مرکز بارگذاری کلید اولیه جهت تضمین صحت اجزاء مربوط به امنیت HSM فراهم کند.

الزام E7: هر دستگاه باید یک شناسه منحصر به فرد قابل مشاهده و چسبیده به آن داشته باشد.

الزام E8: فروشنده باید یک راهنمای کاربر شامل دستورالعمل مدیریت عملیاتی HSM فراهم نماید، که شامل دستورالعمل ثبت چرخه کل حیات اجزاء مربوط به امنیت HSM و شیوه یکپارچه‌سازی این اجزا در یک دستگاه HSM است. به عنوان مثال:

- اطلاعات تولید و شخصی‌سازی
- حدود زمانی / فیزیکی
- تعمیر و نگهداری
- عزل عملیات
- مفقودی یا سرقتی

فصل ۵

استاندارد رمزگذاری نقطه به نقطه PCI P2PE

(Point-to-Point Encryption)

مقدمه

مخفف Point-to-Point Encryption است. استاندارد رمزگذاری نقطه به نقطه یا نظیر به نظیر (P2PE) مجموعه‌ای جامع از الزامات امنیتی را برای ارائه‌دهندگان راهکار P2PE جهت اعتباربخشی به راهکار P2PE خود و کاهش دامنه PCI DSS برای آنها فراهم می‌کند. P2PE یک برنامه عملکرد متقابل در استاندارد PTS، PA-DSS، PCI DSS و استاندارد امنیت PCI PIN است.

طبق این استاندارد دو ناحیه پرداخت تعریف گردیده است یکی ناحیه شرکت ارائه‌دهنده خدمات پرداخت و کارت می‌باشد و دیگری ناحیه نقطه پایانه پذیرش تا نقطه پردازش

تراکنش در ناحیه شرکت ارائه‌دهنده خدمات پرداخت می‌باشد. براساس این استاندارد، اطلاعات تراکنش از ابتدا (کارت خوان MPOS) تا PSP به صورت رمزنگاری‌شده منتقل می‌گردد.

استاندارد P2PE اصول امنیتی ذیل را در راهکار خود بیان داشته است:

- رمزنگاری امن داده‌های کارت در point-of-interaction (POI)
- برنامه‌های مورد تایید P2PE در POI
- مدیریت امن دستگاه‌های مربوط به رمزنگاری
- مدیریت محیطی که داده‌ها در آن رمزگشایی می‌گردند و تمامی داده‌های رمزگشایی‌شده
- استفاده از متدولوژی‌های رمزنگاری امن و عملیات‌های مربوط به کلیدهای رمزنگاری شامل تولید کلید، انتقال، کلیدگذاری، مدیریت و استفاده از کلیدها

این استاندارد به منظور آسان نمودن پیاده‌سازی راهکارهای (P2PE) در نظر گرفته شده که باعث می‌شود داده‌های کارت پرداخت هنگامی که به چنگ مهاجمان می‌افتند، کم‌ارزش شوند.

با استفاده از (P2PE)، یک راهکار رمزنگاری نقطه به نقطه (نظیر به نظیر)، اطلاعات حساب را از نقطه‌ای که پذیرنده، کارت پرداخت را استفاده می‌کند، حفاظت می‌کند و اطلاعات حساب (اطلاعات دارنده کارت و اطلاعات احراز هویت حساس) تا زمانی که به محیط رمزگشایی امن برسد (که این محیط، داده‌ها را هنگامی که توسط یک آسیب‌پذیری به سرقت می‌روند، کم ارزش می‌کند)، قابل خواندن نیست.

انواع ارائه‌دهندگان راهکار

- ارائه‌دهنده راهکار P2PE

ارائه‌دهنده راهکار P2PE یک نهاد با یک رابطه شخص ثالث بر حسب مشتریان پذیرنده خود (به عنوان مثال، یک پردازنده، بانک پذیرنده و یا درگاه پرداخت) است که مسئولیت کلی برای طراحی و پیاده‌سازی یک راهکار خاص P2PE، و مدیریت راهکار P2PE را

برای مشتریان پذیرنده خود دارد. ارائه‌دهنده راهکار مسئولیت کلی برای تضمین الزامات P2PE، از جمله تمام الزامات P2PE انجام‌شده توسط نهادهای شخص ثالث به نمایندگی از ارائه‌دهنده راهکار (به عنوان مثال، سازمان‌های صدور گواهینامه و مراکز تزریق کلید) را دارد.

- پذیرنده به عنوان ارائه‌دهنده راهکار / راهکار مدیریت‌شده توسط پذیرنده (MMS[1])

اصطلاحات " پذیرنده به عنوان ارائه‌دهنده راهکار" و " راهکار مدیریت‌شده توسط پذیرنده"، به پذیرندگانی اطلاق می‌شود که به جای برون‌سپاری راهکار به یک ارائه‌دهنده راهکار P2PE شخص ثالث، راهکارهای P2PE مربوط به خود را به نمایندگی از محیط رمزگذاری پذیرنده مربوط به خودشان مدیریت می‌کنند.

دستگاه‌های رمزنگاری امن (SCD[2]):

دستگاه‌های رمزنگاری امن (SCD) برای رمزگذاری و رمزگشایی داده‌های حساب کاربری، و همچنین برای ذخیره‌سازی و مدیریت کلیدهای رمزنگاری استفاده می‌شود. SCDها شامل دستگاه‌های بارگذاری کلید (KLD[3])، دستگاه‌های رمزگذاری نقطه تعامل (POI[4])، و ماژول‌های امنیتی سخت‌افزار (HSM[5]) است. SCD مورد استفاده برای پذیرش و رمزگذاری داده‌های حساب کاربری در پایانه فروش بایستی دستگاه POI مورد تایید PCI (PCI PTS) و شامل SRED (خواندن و تبادل امن اطلاعات) باشد. HSMهای مورد استفاده در محیط رمزگشایی برای رمزگشایی داده‌های حساب و عملیات کلید رمزنگاری مرتبط باید مورد تایید FIPS PUB 140-2 (سطح ۳ یا بالاتر) و یا استاندارد PCI HSM باشد.

[1] Merchant-Managed Solution
[2] Secure Cryptographic Device
[3] Key-Loading Device
[4] Point Of Interaction
[5] Hardware Security Module

نکته: برای راهکارهای P2PE که از رمزنگاری ترکیبی[1] استفاده می‌کنند، SCDها برای رمزگذاری اطلاعات حساب و همچنین برای ذخیره‌سازی و مدیریت کلیدهای رمزنگاری استفاده می‌شود، اما برای رمزگشایی اطلاعات حساب مورد نیاز نیست.

راهکار های P2PE: رمزگشایی سخت‌افزاری و یا رمزگشایی ترکیبی

برای راهکارهای PCI P2PE، محیط رمزگذاری در نقطه پذیرش پذیرنده فقط شامل رمزگذاری سخت‌افزاری در دستگاه‌های POI مورد تایید PCI است.

محیط رمزگشایی PCI P2PE برای مدیریت همه کلیدهای رمزنگاری نیاز به HSMها دارد، و برای رمزگشایی داده‌های حساب (رمزگشایی سخت‌افزاری) از HSMها استفاده شده و یا رمزگشایی داده‌های حساب می‌تواند در خارج از HSM و سیستم‌های میزبان غیر SCD رخ دهد (رمزگشایی ترکیبی).

نکته: رمزگشایی ترکیبی برای راهکار مدیریت‌شده توسط پذیرنده استفاده نمی‌شود.

[1] Hybrid Decryption

حوزه‌ها و الزامات استاندارد P2PE

۱) حوزه‌های P2PE

این استاندارد، دارای شش حوزه است که این حوزه‌ها نشان‌دهنده مناطق اصلی است که در آن کنترل امنیتی باید به کار رفته و اعتبارسنجی شود.

جدول ۵-۱: حوزه‌های استاندارد PCI P2PE

حوزه	توصیف
حوزه ۱: مدیریت دستگاه و برنامه کاربردی رمزگذاری	مدیریت امن دستگاه‌های POI مورد تایید PCI و نرم‌افزار آن.
حوزه ۲: امنیت برنامه کاربردی	توسعه امن برنامه‌های کاربردی پرداخت طراحی شده برای دسترسی به داده‌های حساب متن واضح، صرفا برای نصب در دستگاه‌های POI مورد تایید PCI در نظر گرفته شود.
حوزه ۳: مدیریت راهکار P2PE	مدیریت کلی راهکار P2PE توسط ارائه‌دهنده راهکار، از جمله روابط شخص ثالث، پاسخ رویداد، و راهنمای دستورالعمل P2PE (PIM[1]).
حوزه ۴: راهکار مدیریت-شده توسط پذیرنده	وظایف و قابلیت‌های جداگانه بین محیط‌های رمزنگاری و رمزگشایی پذیرنده.
حوزه ۵: محیط رمزگشایی	مدیریت امن محیطی که داده‌های حساب رمزشده را گرفته و آن را رمزگشایی می‌کند.
حوزه ۶: مدیریت عملیات و دستگاه کلید رمزگذاری P2PE	تاسیس و اداره عملیات مدیریت کلید برای دستگاه‌های POI رمزگذاری داده‌های حساب و HSMهای رمزگشایی.

۲) کاربرد حوزه‌ها برای ارزیابی دستگاه SCD

راهکارهای P2PE نیاز به استفاده از انواع مختلف SCD دارد. برای کمک به ارزیابی انواع مختلف دستگاه، ماتریس زیر حوزه‌های هر نوع SCD را نشان می‌دهد:

[1] P2PE Instruction Manual

جدول ۵-۲: کاربرد حوزه‌ها برای ارزیابی دستگاه SCD

حوزه	نوع و کاربرد SCD		
	دستگاه POI مورد تایید PCI برای رمزگذاری داده حساب	FIPS[1] 140-2 سطح ۳ و یا HSM مورد تایید PCI برای رمزگشایی داه حساب	SCD برای تزریق کلید رمزنگاری یا عملیات کلید
۱	قابل اجرا	N/A	N/A
۲	N/A	N/A	N/A
۳	N/A	N/A	N/A
۴	N/A	N/A	N/A
۵	N/A	قابل اجرا	N/A
۶	قابل اجرا	قابل اجرا	قابل اجرا

۳) ارتباط حوزه‌ها با نهادهای ارائه‌دهنده خدمات P2PE

حوزه‌های P2PE بر اساس عملکردهای مختلف (الزامات P2PE) گروه‌بندی شده و به شرح جدول زیر با نهادهای ارائه‌دهنده خدمات P2PE مرتبط می‌گردد:

[1] Federal Information Processing Standards

جدول ۵-۳: ارتباط حوزه‌ها با نهادهای ارائه‌دهنده خدمات P2PE

حوزه	نهاد تحت اعتبارسنجی P2PE
۱	• ارائه‌دهنده راهکار یا • پذیرنده به عنوان ارائه‌دهنده راهکار یا • ارائه‌دهنده اجزای خدمات مدیریت رمزگذاری
۲	• ارائه‌دهنده راهکار یا • پذیرنده به عنوان ارائه‌دهنده راهکار یا • فروشنده برنامه کاربردی P2PE
۳	• ارائه‌دهنده راهکار یا • پذیرنده به عنوان ارائه‌دهنده راهکار
۴	• پذیرنده به عنوان ارائه‌دهنده راهکار
۵	• ارائه‌دهنده راهکار یا • پذیرنده به عنوان ارائه‌دهنده راهکار یا • ارائه‌دهنده اجزای خدمات مدیریت رمزگشایی
۶	• ارائه‌دهنده راهکار یا پذیرنده به عنوان ارائه‌دهنده راهکار و/یا • ارائه‌دهنده اجزای خدمات مدیریت رمزگذاری یا رمزگشایی و/یا • ارائه‌دهنده اجزای خدمات KIF یا CA/RA

٤) دامنه ارزیابی راهکارهای P2PE

دامنه ارزیابی راهکار P2PE، شش حوزه P2PE را به عنوان بخشی از ارزیابی P2PE کامل ارائه‌دهنده راهکار و یا به عنوان نتیجه تجمیعی یک یا چند ارزیابی مستقل اجزا P2PE یا برنامه‌های کاربردی P2PE پوشش می‌دهد.

جدول ۵-۴: دامنه ارزیابی راهکارهای P2PE

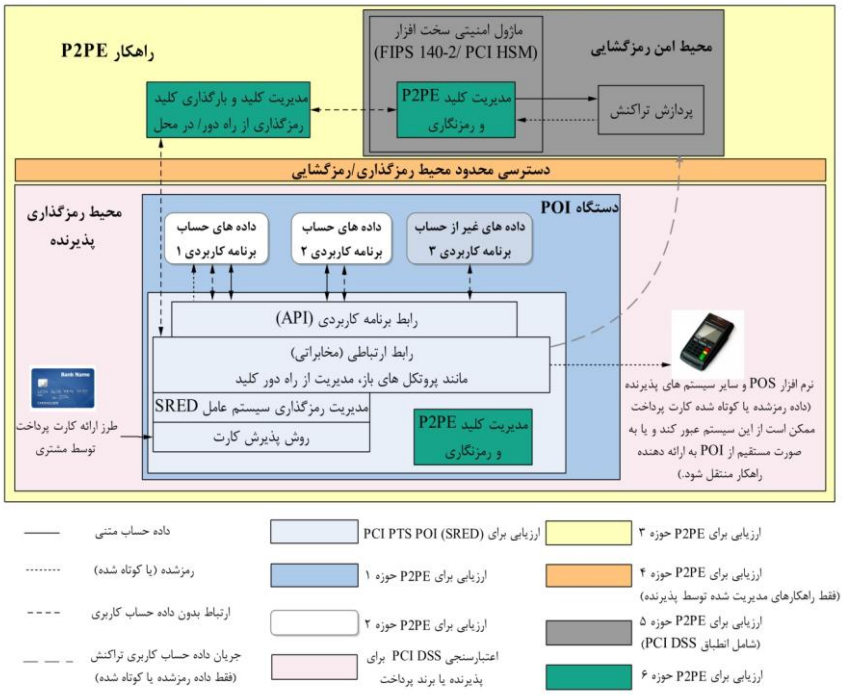
حوزه	دامنه ارزیابی
۱	• تمام دستگاه‌های POI مورد تایید PCI قرارگرفته در راهکار P2PE (برای پذیرنده به منظور استفاده برای پذیرش پرداخت). • ادغام تمام نرم‌افزارها بر روی دستگاه‌های POI ▪ برنامه‌های کاربردی پرداخت P2PE (برای ارزیابی دامنه ۲) ▪ نرم‌افزار غیرپرداختی P2PE (با عدم دسترسی به متن واضح داده حساب به عنوان مثال، برنامه کاربردی وفاداری و یا تبلیغاتی)
۲	• برای نرم‌افزارهای مورد استفاده در دستگاه‌های POI با دسترسی به متن واضح داده حساب
۳	نکته: این دامنه نمی‌تواند به شخص ثالث و یا ارائه‌دهنده اجزاء P2PE برون‌سپاری شود و **باید** توسط ارائه‌دهنده راهکار P2PE (و یا پذیرنده به عنوان ارائه‌دهنده راهکار) اجرا شود. • مدیریت کلی ارائه‌دهنده راهکار P2PE از جمله روابط شخص ثالث، ارتباطات بین نهادهای مختلف P2PE، و / یا استفاده از ارائه‌دهندگان اجزاء P2PE. • راهنمای دستورالعمل P2PE (PIM) متمرکز بر پذیرنده که ارائه‌دهنده راهکار آن را تهیه و بین پذیرندگان (برای محیط رمزنگاری خود) توزیع می‌کند، از جمله تکمیل الگوی PIM ارائه‌شده PCI.
۴	• تعیین الزامات برای تفکیک بین محیط رمزگذاری پذیرنده و محیط رمزگشایی پذیرنده.
۵	• مدیریت تمامی اجزای سیستم واقع و یا متصل به محیط رمزگشایی، از جمله اجزای مورد استفاده برای رمزگشایی داده حساب، و • حفظ انطباق PCI DSS برای محیط رمزگشایی.
۶	• مدیریت امن کلید - از جمله تمام HSMها، دستگاه‌های بارگذاری کلید، و غیره - توسط ارائه‌دهنده راهکار و یا شخص ثالث که برای عملیات کلید رمزنگاری در حمایت از دستگاه‌های POI رمزگذاری داده حساب (حوزه ۱) و HSMهای رمزگشایی (حوزه ۵) استفاده می‌شود.

۵) ارتباط میان P2PE و سایر استانداردهای PCI (PCI DSS, PA-DSS, PTS POI, and PIN)

- دستگاه‌های POI (برای رمزگذاری داده‌های حساب) که به ازای هر یک از الزامات نقطه تعامل (POI) امنیت تراکنش احراز هویت (PTS) تایید شده‌اند.
- HSMهای محیط رمزگشایی (برای رمزگشایی داده‌های حساب و عملیات کلید رمزنگاری مرتبط) که به ازای هر یک از الزامات PCI PTS HSM (یا FIPS 140-2 سطح ۳) تایید شده‌اند.
- عملیات کلید رمزنگاری برای محیط‌های رمزگذاری و رمزگشایی با استفاده از شیوه‌های مدیریت کلید ناشی از استاندارد امنیت PTS PIN.
- برنامه‌های کاربردی در دستگاه‌های POI با دسترسی به متن واضح داده‌های ناشی از استاندارد امنیت داده برنامه کاربردی پرداخت (PA-DSS).
- محیط رمزگشایی با PCI DSS انطباق دارد.

۶) پیاده‌سازی P2PE در یک نگاه

دیاگرام زیر پیاده‌سازی عمومی P2PE و ارتباط هر یک از حوزه‌های استاندارد در هر ناحیه را نشان می‌دهد. (این شکل نمونه‌ای از یک نوع سناریو می‌باشد.)



شکل ۵-۱: پیاده‌سازی P2PE در یک نگاه

۷) الزامات حوزه ۱: مدیریت دستگاه و برنامه کاربردی رمزگذاری

1A: داده‌های حساب باید در تجهیزات مقاوم در برابر مصالحه فیزیکی و منطقی رمزگذاری شود.

الزام 1A-1: دستگاه های POI مورد تایید PCI با SRED برای پذیرش تراکنش استفاده شود.

الزام 1A-2: برنامه‌های کاربردی دستگاه‌های POI با دسترسی به متن واضح داده‌های حساب قبل از استقرار در راهکار P2PE به ازای حوزه ۲ ارزیابی شود.

1B: دستگاه‌های POI امن از لحاظ منطقی.

الزام 1B-1: ارائه‌دهنده راهکار، دسترسی منطقی به دستگاه‌های POI مستقر در محیط رمزگذاری پذیرنده را در اختیار پرسنل مجاز قرار دهد.

الزام 1B-2: ارائه‌دهنده راهکار، دسترسی از راه دور به دستگاه‌های POI مستقر در محیط رمزگذاری پذیرنده را امن نماید.

الزام 1B-3: ارائه‌دهنده راهکار، روش‌های محافظت از دستگاه‌های POI و برنامه‌های کاربردی از آسیب‌پذیری‌های شناخته‌شده را پیاده‌سازی نموده و دستگاه‌ها را به صورت امن به‌روزرسانی کند.

الزام 1B-4: ارائه‌دهنده راهکار، روش‌های تامین امنیت داده‌های حساب در هنگام عیب‌یابی را پیاده‌سازی نماید.

الزام 1B-5: راهکار P2PE، Log واضحی از تمام تغییرات قابلیت‌های مهم دستگاه POI ارائه دهد.

1C: استفاده از برنامه‌های کاربردی P2PE که از PAN و SAD محافظت کند.

الزام 1C-1: برنامه‌های کاربردی در هنگام استفاده از منابع به اشتراک گذاشته و به‌روزرسانی برنامه‌ها و قابلیت‌های آن به صورت امن اجرا شود.

الزام 1C-2: برنامه‌های کاربردی و یا نرم‌افزارهایی که مورد نیاز کسب‌وکار نیست، نباید به داده‌های حساب دسترسی داشته باشد.

1D: پیاده‌سازی فرآیندهای مدیریت برنامه‌های کاربردی امن.

الزام 1D-1: یکپارچگی برنامه‌های کاربردی در طول نصب و و به‌روزرسانی آن حفظ شود.

الزام 1D-2: اسناد و مدارک و برنامه‌های آموزشی برای نصب و راه‌اندازی، تعمیر و نگهداری / ارتقاء و به‌روزرسانی، و استفاده از برنامه‌های کاربردی ایجاد شود.

1E: فقط ارائه‌دهندگان اجزا: وضعیت گزارش به ارائه‌دهندگان راهکار.

الزام 1E-1: کنترل P2PE بحرانی، برای ارائه‌دهندگان اجزای خدمات مدیریت رمزگذاری، برقرار و مانیتور شده و برای ارائه‌دهندگان راهکار معتبر و مسئول گزارش شود.

۸) الزامات حوزه ۲: امنیت برنامه کاربردی

2A: محافظت از PAN و SAD.

الزام 2A-1: برنامه کاربردی در دستگاه POI مورد تایید PCI با SRED فعال اجرا شود.

الزام 2A-2: برنامه کاربردی PAN و / یا SAD را به جز در فرآیندهای مورد نیاز کسب‌وکار ذخیره نکند.

الزام 2A-3: برنامه کاربردی PAN و / یا SAD متن واضح را به بیرون از دستگاه POI انتقال نداده و تنها از روش‌های ارتباطی حوزه ارزیابی دستگاه POI مورد تایید PCI استفاده کند.

2B: توسعه و نگهداری برنامه‌های کاربردی امن.

الزام 2B-1: برنامه کاربردی طبق شیوه‌های استاندارد صنعت چرخه حیات توسعه نرم-افزار و امنیت اطلاعات توسعه می‌یابد.

الزام 2B-2: برنامه کاربردی بایستی به صورت امن اجرا شود، از جمله استفاده امن از هر گونه منابع مشترک میان برنامه‌های کاربردی مختلف.

الزام 2B-3: فروشنده برنامه کاربردی از پروتکل‌های امن استفاده نموده، راهنمای استفاده از آن را فراهم نموده، و تست یکپارچه‌سازی در برنامه کاربردی نهایی انجام می‌دهد.

الزام 2B-4: برنامه‌های کاربردی هیچ توابع رمزگذاری به جای رمزگذاری SRED اجرا نمی‌کنند. همه توابع توسط (سفت‌افزار) سیستم عامل SRED تاییدشده دستگاه POI انجام می‌شود.

2C: پیاده‌سازی فرآیندهای مدیریت برنامه‌های کاربردی امن.

الزام 2C-1: آسیب‌پذیری‌های جدید کشف شده و برنامه‌های کاربردی برای آن آسیب-پذیری‌ها به صورت مداوم تست می‌شود.

الزام 2C-2: برنامه‌های کاربردی تنها از طریق فرآیندهای قابل اعتماد، تصدیق شده و رمزنگاری شده و با استفاده از یک مکانیزم امنیتی تایید شده برای دستگاه POI مورد تایید PCI، نصب شده و بروزرسانی‌ها اجرا شود.

الزام 2C-3: اسناد و مدارک و برنامه‌های آموزشی برای نصب و راه‌اندازی، تعمیر و نگهداری / ارتقاء و به‌روزرسانی، و استفاده از برنامه‌های کاربردی ایجاد شود.

۹) الزامات حوزه ۳: مدیریت راهکار P2PE

3A: مدیریت راهکار P2PE.

الزام 3A-1: ارائه‌دهنده راهکار اسناد و مدارک جزئیات معماری راهکار P2PE و جریان داده‌ها را نگهداری نماید.

الزام 3A-2: ارائه‌دهنده راهکار گزارش وضعیت ارائه‌دهندگان اجزای P2PE را مدیریت و مانیتور کند.

الزام 3A-3: ارائه‌دهنده راهکار فرآیندهای پاسخ‌دهی به پیغام‌های پذیرندگان، ارائه-دهندگان اجزاء، و / یا اشخاص ثالث را اجرا نموده و در مورد هر گونه فعالیت مشکوک حوزه راهکار P2PE پیغامی را ارائه نماید.

الزام 3A-4: اگر راهکار اجازه توقف رمزگذاری P2PE داده‌های حساب کاربری را به پذیرنده دهد، ارائه‌دهنده راهکار بایستی فرآیندهای مربوطه را برای پذیرندگان مدیریت نماید.

3B: مدیریت شخص ثالث.

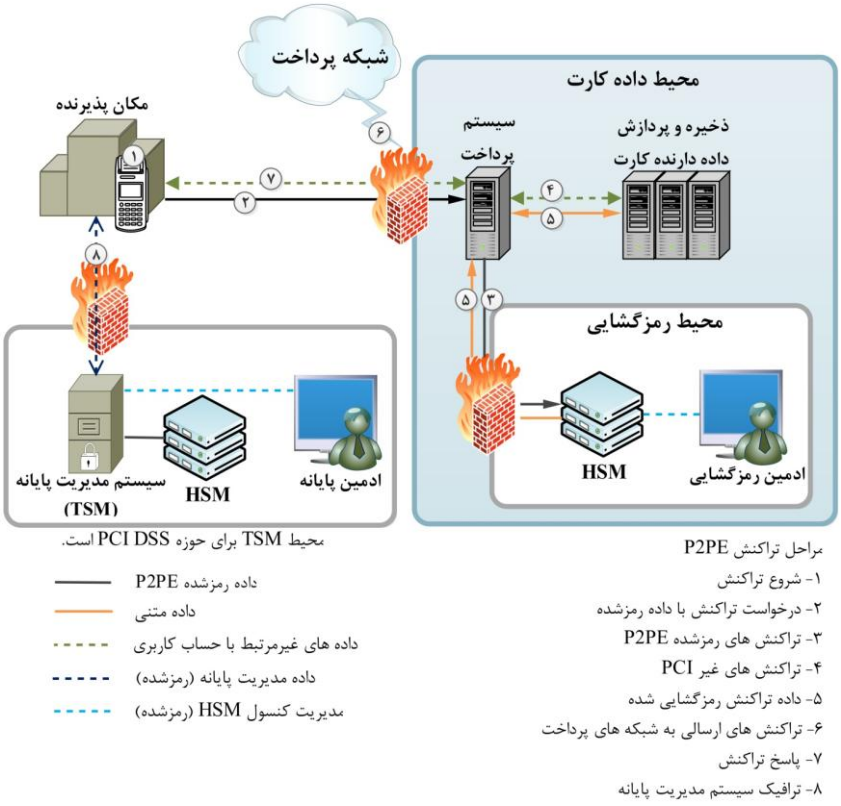
الزام 3B-1: ارائه‌دهنده راهکار باید یک توافقنامه رسمی با تمام اشخاص ثالث برای عقد قرارداد جهت انجام قابلیت‌های P2PE به نمایندگی از ارائه‌دهنده راهکار تسهیل و برقرار نماید.

3C: ایجاد و نگهداری از راهنمای دستورالعمل P2PE برای پذیرنده‌ها.

الزام 3C-1: ارائه‌دهنده راهکار یک راهنمای دستورالعمل P2PE (PIM) برای پذیرندگان توسعه، حفظ، و منتشر کند.

۱۰) الزامات حوزه ٤: راهکار مدیریت‌شده توسط پذیرنده: جداسازی محیط رمزگذاری و رمزگشایی پذیرنده

مثالی از جداسازی محیط رمزگذاری و رمزگشایی پذیرنده برای راهکار مدیریت‌شده توسط پذیرنده به شکل زیر است:



شکل ۵-۲: جداسازی محیط رمزگذاری و رمزگشایی پذیرنده

4A: مدیریت راهکار P2PE.

الزام 4A-1: محیط رمزگشایی پذیرنده باید برای عملیات رمزگشایی اختصاص یابد.

الزام 4A-2: دسترسی به محیط رمزگشایی پذیرنده و سایر شبکه‌ها / سیستم‌ها محدود شود.

4B: مدیریت شخص ثالث.

الزام 4B-1: ترافیک بین محیط رمزگذاری و سایر CDE[1]ها (محیط‌های داده دارنده کارت) محدود شود.

4C: ایجاد و نگهداری راهنمای دستورالعمل P2PE برای پذیرنده‌ها.

الزام 4C-1: پرسنل داخلی پذیرنده (محیط رمزگذاری) دسترسی منطقی به محیط رمزگشایی، سایر CDEها، و یا کلیدهای رمزگشایی داده حساب نداشته باشد.

۱۱) الزامات حوزه ۵: محیط رمزگشایی

5A: استفاده از دستگاه‌های رمزگشایی مورد تایید.

الزام 5A-1: از دستگاه‌های رمزگشایی مورد تایید استفاده گردد.

5B: محیط رمزگشایی امن شود.

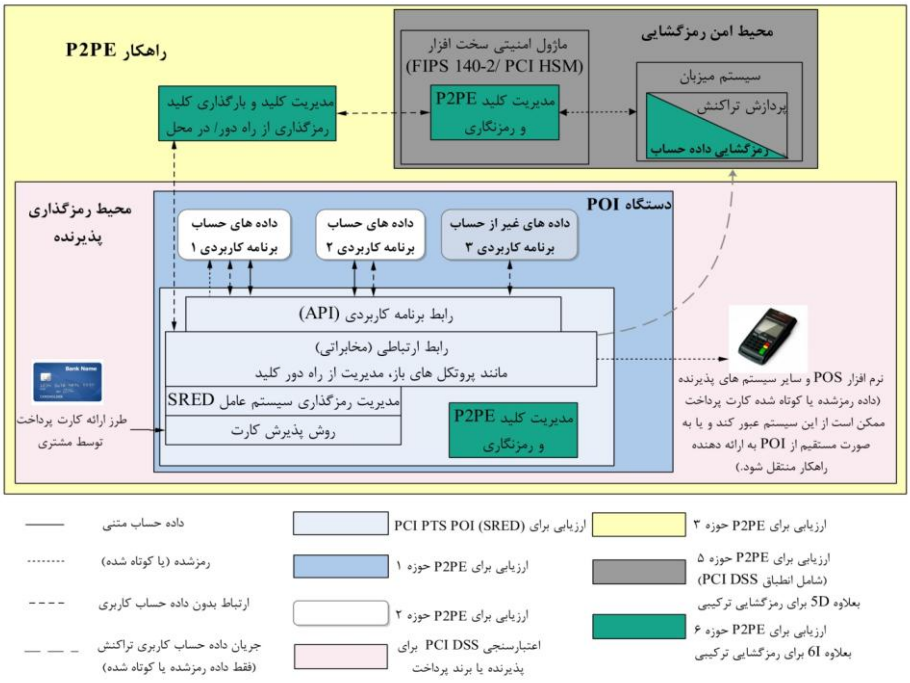
الزام 5B-1: فرآیندهای مدیریت امن محیط رمزگشایی برقرار شود.

5C: مانیتورینگ محیط رمزگشایی و پاسخ به رویدادها.

الزام 5C-1: رویدادها ثبت و محیط رمزگشایی برای فعالیت‌های مشکوک مانیتور شده، و فرآیندهای پیغام و اطلاع‌رسانی پیاده‌سازی گردد.

[1] Cardholder Data Environment

5D: پیاده‌سازی فرآیندهای رمزگشایی امن و ترکیبی.



شکل ۵-۳: پیاده‌سازی رمزگشایی ترکیبی P2PE

الزام 5D-1: سیستم میزبان به صورت امن پیکربندی شود.

الزام 5D-2: کنترل دسترسی برای سیستم میزبان به صورت امن پیکربندی شود.

الزام 5D-3: دسترسی‌های غیرکنسول به سیستم میزبان به صورت امن پیکربندی شود.

الزام 5D-4: محیط فیزیکی سیستم میزبان ایمن شود.

5E: فقط ارائه‌دهندگان اجزا: وضعیت گزارش به ارائه‌دهندگان راهکار.

الزام 5E-1: کنترل P2PE بحرانی، برای ارائه‌دهندگان اجزای خدمات مدیریت رمزگذاری، برقرار و مانیتور شده و برای ارائه‌دهندگان راهکار معتبر و مسئول گزارش شود.

۱۲) الزامات حوزه ٦: مدیریت عملیات و دستگاه کلید رمزگذاری P2PE

6A: داده‌های حساب با استفاده از الگوریتم‌ها و روش‌هایی پردازش شود که نگهداری امن آنها تضمین گردد.

الزام 6A-1: داده حساب با الگوریتم‌های رمزنگاری، اندازه و قدرت کلیدها و فرآیندهای مدیریت کلید مناسب محافظت شود.

6B: کلیدهای داده‌های حساب و روش‌های مدیریت کلید با استفاده از فرآیندهایی ایجاد شود که امکان پیش‌بینی کلید و یا تعیین کلیدی خاص محتمل‌تر از بقیه کلیدها نباشد.

الزام 6B-1: همه کلیدها و مولفه‌های کلید با استفاده از یک فرآیند تصادفی یا شبه-تصادفی تاییدشده تولید شود.

الزام 6B-2: توافق بر روی فرآیند تولید کلید نباید بدون تبانی بین حداقل دو نفر مورد اعتماد امکان‌پذیر باشد.

الزام 6B-3: روش‌های مستندسازی باید وجود داشته و آشکارا در تمام پردازش‌های تولید کلید استفاده شود.

6C: کلیدها به شیوه‌ای امن منتقل شود.

الزام 6C-1: کلیدهای محرمانه و یا خصوصی باید به شرح ذیل انتقال یابد:

- الف) انتقال فیزیکی کلید با حداقل دو بخش جداگانه کلید و یا کل کلید (چاپ، کارت‌های هوشمند، SCD) با استفاده از کانال‌های ارتباطی مختلف، و یا
- ب) انتقال کلید در قالب متن رمزشده.

کلیدهای عمومی باید با حفظ تمامیت و صحت آن منتقل شود.

الزام 6C-2: در طول ارسال، انتقال، یا حرکت بین دو نهاد سازمانی، هر یک از اجزای کلید محرمانه و یا خصوصی رمزنشده باید همیشه محافظت شود.

الزام 6C-3: همه کلیدهای رمزنگاری کلید مورد استفاده برای انتقال و یا ارسال سایر کلیدهای رمزنگاری باید (حداقل) به اندازه کلیدهای منتقل‌شده و یا ارسال‌شده قوی باشد.

الزام 6C-4: روش‌های مستندسازی باید وجود داشته و آشکارا در تمام پردازش‌های ارسال و یا انتقال کلید استفاده شود.

6D: بارگذاری کلید به شیوه‌ای امن مدیریت شود.

الزام 6D-1: کلیدهای محرمانه و خصوصی باید به صورت امن وارد ماژول‌های امنیتی سخت‌افزار (میزبان) (HSM) و دستگاه‌های نقطه تعامل (POI) شود.

- الف) کلیدهای محرمانه و خصوصی باید با استفاده از اصول کنترل دوگانه و دانش دوبخشی وارد دستگاه‌های رمزنگاری شود.
- ب) تکنیک‌های استقرار کلید باید با استفاده از رمزنگاری کلید عمومی و به صورت امن اجرا شود.

الزام 6D-2: مکانیسم مورد استفاده برای بارگذاری کلیدهای محرمانه و خصوصی - مانند پایانه‌ها، PIN PADهای خارجی، key gunها، و یا دستگاه‌ها و روش‌های مشابه - جهت جلوگیری از هرگونه مانیتورینگ برآمده از افشای غیرمجاز هر یک از اجزا باید محافظت شود.

الزام 6D-3: تمام سخت‌افزار و مکانیزم‌های دسترسی / احراز هویت (به عنوان مثال، کلمات عبور) مورد استفاده برای بارگذاری کلید و یا امضای برنامه‌های کاربردی مجاز (به عنوان مثال، برای "لیست سفید (مجاز)") باید تحت کنترل دوگانه مدیریت شود.

الزام 6D-4: بارگذاری کلید و یا اجزای کلید باید با یک مکانیزم اعتبارسنجی ترکیب شود، به طوری که صحت کلید تضمین شده و به طور قطع نتواند در معرض دستکاری، جایگزینی، و یا خطر باشد.

الزام 6D-5: روش‌های مستندسازی باید وجود داشته و آشکارا در تمام فعالیت‌های بارگذاری کلید (از جمله audit trail) استفاده شود.

6E: کلیدها به شیوه‌ای استفاده شود که استفاده غیرمجاز را تشخیص و جلوگیری نماید.

الزام 6E-1: کلیدهای رمزنگاری منحصربه‌فرد و مخفی باید برای هر لینک شناسایی بین سیستم‌های کامپیوتر میزبان دو سازمان یا سیستم‌های منطقی جداگانه در همان سازمان استفاده شود.

الزام 6E-2: روش‌هایی برای جلوگیری و یا تشخیص تعویض‌های غیرمجاز یک کلید با کلید دیگر (جایگزین و سوءاستفاده غیرمجاز کلید) و یا عملکرد دستگاه رمزنگاری بدون کلید مشروع باید وجود داشته باشد.

الزام 6E-3: کلیدهای رمزنگاری باید فقط برای هدف مدنظر خود استفاده شود و هرگز نباید بین سیستم‌های تولید و تست به اشتراک گذاشته‌شود.

الزام 6E-4: کلیدهای رمزنگاری محرمانه و خصوصی موجود و مورد استفاده برای هر قابلیت (به عنوان مثال، رمزنگاری کلید و یا رمزنگاری داده حساب) توسط دستگاه POI که داده حساب را پردازش می‌نماید، باید منحصر به فرد (مگر در حالت تصادفی) برای آن دستگاه باشد.

6F: کلیدها به شیوه‌ای امن اداره شود.

الزام 6F-1: کلیدهای محرمانه مورد استفاده برای رمزنگاری کلید رمزگذاری داده حساب و یا برای رمزگذاری داده حساب، و یا کلیدهای خصوصی مورد استفاده در ارتباط با پیاده‌سازی توزیع از راه دور کلید، هرگز نباید خارج از SCDها وجود داشته باشند، به جز زمانی که رمزگذاری شده و یا به صورت امن ذخیره و با استفاده از اصول کنترل دوگانه و دانش دوبخشی مدیریت شود.

الزام 6F-2: روش‌های جایگزینی کلیدهای در معرض شناخته شدن و یا مشکوک با کلیدهای فرعی (رمزگذاری شده توسط کلیدهای در خطر) باید وجود داشته و آشکارا استفاده شود. همچنین کلیدهای حاصله از کلید در خطر، مرتبط با کلید اصلی نباشد.

الزام 6F-3: کلیدهایی که با استفاده از روش‌های محاسبه کلید برگشت‌پذیر تولید می‌شوند، مانند سایر انواع کلیدها، تنها باید در SCDهای دارای کلید اصلی استفاده شوند.

کلیدهایی که با استفاده از روش‌های محاسبه کلید برگشت‌پذیر تولید می‌شوند، نباید در سطوح مختلف سلسله مراتب کلید استفاده شوند. به عنوان مثال، یک نوع از یک کلید رمزنگاری کلید مورد استفاده برای تبادل کلید نباید به عنوان یک کلید کار یا به عنوان یک کلید فایل اصلی برای ذخیره‌سازی محلی استفاده شود. کلیدهایی که با یک فرآیند غیرقابل برگشت تولید می‌شوند، مانند فرآیند اشتقاق و یا تبدیل کلید با یک کلید پایه با استفاده از فرآیند رمزنگاری، مشمول این الزامات نیست.

الزام 6F-4: کلیدها و اجزای کلید محرمانه و خصوصی که مدتی مورد استفاده قرار نگیرد و یا جایگزین شده باشد باید به صورت امن نابود شود.

الزام 6F-5: دسترسی به کلیدها و مواد کلید رمزنگاری محرمانه و خصوصی باید:

- الف) بر اساس نیاز به دانش محدود شود، به طوری که کمترین تعداد متولیان کلید برای استفاده موثر فعال شوند؛ و
- ب) حفاظت شود به طوری که هیچ فرد دیگری نتواند مشاهده و یا اجزای آن را کسب کند.

الزام 6F-6: Log ها باید در مواقعی که کلیدها، اجزای کلید، و یا مواد مرتبط از حافظه حذف شده و یا در SCD بارگذاری می‌شود، نگهداری گردد.

الزام 6F-7: پشتیبان‌گیری از کلیدهای محرمانه و خصوصی باید تنها به منظور تثبیت و نصب دوباره کلیدهایی که به طور تصادفی از بین رفته و یا غیر قابل دسترس شده‌اند، وجود داشته باشد. پشتیبان‌گیری باید تنها در یکی از قالب‌های ذخیره‌سازی مجاز برای آن کلید باشد.

الزام 6F-8: روش‌های مستندسازی باید وجود داشته و آشکارا در تمام فعالیت‌های مدیریت کلید استفاده شود.

6G: تجهیزات مورد استفاده برای پردازش داده‌ها و کلیدهای حساب به شیوه‌ای امن مدیریت شود.

الزام 6G-1: تجهیزات مورد استفاده برای محافظت از اطلاعات حساب کاربری (به عنوان مثال، دستگاه های POI و HSMها) باید تنها در صورتی در اختیار سرویسی قرار داده شود که تضمین آن وجود دارد که آن تجهیزات تعویض نشده و یا در معرض تغییرات غیرمجاز و یا tampering قبل از استقرار دستگاه وجود ندارد - هم قبل و هم پس از بارگذاری کلیدهای رمزنگاری - و اقدامات احتیاطی برای به حداقل رساندن تهدید در زمان استقرار انجام شده باشد.

الزام 6G-2: حفاظت فیزیکی و منطقی باید برای دستگاه های POI مستقر وجود داشته باشد.

الزام 6G-3: روشی برای محافظت از هر SCD - برای اطمینان از نابودی همه کلیدهای رمزنگاری و یا اجزای کلید در این دستگاه‌ها — در زمان خروج از سرویس، اتمام چرخه حیات استقرار، یا بازگشت برای تعمیر باید در محل وجود داشته و اجرا گردد.

الزام 6G-4: هر SCDای که قادر به رمزنگاری یک کلید و تولید رمز آن کلید (به عنوان مثال، یک HSM یا دستگاه تزریق / بارگذاری کلید)، و یا امضای برنامه‌های کاربردی بارگذاری‌شده بر روی یک دستگاه POI است، باید در برابر استفاده غیرمجاز برای رمزنگاری کلید شناخته شده و یا اجزای کلید شناخته‌شده محافظت شود. این محافظت به یک یا چند شکل زیر انجام می‌شود:

- الف) کنترل دسترسی دوگانه برای فعال نمودن قابلیت رمزنگاری کلید مورد نیاز است،
- ب) حفاظت فیزیکی از تجهیزات (به عنوان مثال، قفل دسترسی به آن) تحت کنترل دوگانه
- ج) جلوگیری از دسترسی منطقی به تجهیزات

الزام 6G-5: روش‌های مستندسازی باید وجود داشته و آشکارا در تضمین امنیت و تمامیت تجهیزات پردازش داده حساب (به عنوان مثال دستگاه های POI و HMSها) در

اختیار سرویس قرار داده شود، مقداردهی شده، استقرار یافته، مورد استفاده قرار گرفته و از رده خارج شود.

6H: برای راهکارهای رمزگشایی ترکیبی: پیاده‌سازی مدیریت امن کلید ترکیبی.

الزام 6H-1: راهکار رمزگشایی ترکیبی، کلیدهای رمزگشایی داده‌ای (DDK) را که داده حساب را در نرم‌افزار سیستم میزبان رمزگشایی می‌کند، به صورت امن مدیریت نماید.

6I: فقط ارائه‌دهندگان اجزا: وضعیت گزارش به ارائه‌دهندگان راهکار.

الزام 6I-1: کنترل P2PE حیاتی برای ارائه‌دهندگان اجزاء که خدمات مدیریت کلید، مدیریت دستگاه و یا مدیریت رمزگشایی انجام می‌دهند، حفظ و مانتیور شده و گزارش آن برای ارائه‌دهنده راهکار مسئول تهیه گردد.

فصل ٦

استاندارد EMV (Europay, MasterCard, Visa)

مقدمه

۱) هدف

هدف از این سند، ارائه یک نمای کلی از مشخصات و فرآیندهای EMV در چارچوب صنعت پرداخت است.

۲) EMV چیست؟

EMV مخفف سه کلمه Europay, MasterCard, Visa است، سه شرکتی که در اصل استاندارد را ایجاد کرد. در حال حاضر این استاندارد توسط EMVCo مدیریت می‌شود. EMVCo کنسرسیومی است که توسط Visa، MasterCard، JCB، American Express، China UnionPay و Discover کنترل می‌شود.

EMV برای عملیات بین کارت‌های هوشمند، دستگاه‌های پایانه فروش قادر به پذیرش کارت هوشمند، دستگاه‌های خودپرداز و همچنین تایید تراکنش‌های کارت نقدی و اعتباری می‌باشد. کارت‌های EMV، (که کارت‌های تراشه یا IC نیز نامیده می‌شوند) کارت‌های هوشمندی هستند که اطلاعات را به جای نوار مغناطیسی بر روی مدار مجتمع، ذخیره می‌کنند. بسیاری از کارت‌های EMV با stripeها نیز سازگاری دارند. این کارت‌ها می‌توانند یا کارت‌های تماسی بوده و بایستی به صورت فیزیکی داخل کارت خوان قرار گیرند، یا کارت‌های بدون تماس باشند که از یک فاصله کوتاه با استفاده از تکنولوژی شناسایی فرکانس رادیویی (RFID) خوانده شوند. در این استاندارد از روش‌های احراز هویت کارت به همراه PIN و پیشگیری از حملات شبیه‌سازی کارت استفاده می‌شود.

هدف از طراحی کارت هوشمند EMV کاهش احتمال وقوع هرگونه سوء استفاده و کلاه برداری از طریق نوار مغناطیسی می‌باشد.

از ویژگی‌های بارز EMV این است که نرم‌افزار پرداخت مصرف کننده در یک تراشه امن تعبیه شده در یک کارت پرداخت پلاستیکی (کارت تراشه یا کارت هوشمند) و یا در یک دستگاه شخصی مانند تلفن همراه قرار گرفته است. تراشه سه عنصر کلیدی را فراهم می‌نماید:

- ذخیره اطلاعات
- انجام پردازش
- ذخیره ایمن اطلاعات محرمانه و انجام پردازش رمزنگاری (تراشه یک عنصر امن است)

به منظور اجرای پرداخت، تراشه باید به یک تراشه خوان در ترمینال پذیرش (attended POS, unattended POS, ATM) به دو صورت تماسی (ارتباط فیزیکی) و یا غیرتماسی (در مجاورت حداکثر ۴ سانتیمتر) ارتباط برقرار کند. در هر دو سناریو، ترمینال پذیرش قدرت پردازش را برای تراشه فراهم می‌نماید. کارت تراشه می‌تواند به صورت تماسی، غیرتماسی و یا هردو باشد. در حالت بدون کارت مانند موبایل فقط نوع غیرتماسی امکان پذیر می‌باشد.

از آنجا که سرویس‌دهندگان بسیاری در سطح جهان خدمات بانکی مرتبط با کارت هوشمند را ارایه می‌کنند، در صورتی که هر یک بخواهند از سیستم خاص خود استفاده کند، امکان اتصال این سیستم‌ها به یکدیگر بسیار مشکل می‌گردد. از این رو شرکت‌های مطرح در این زمینه (Visa, Europay, MasterCard) اقدام به ارایه یک استاندارد واحد با نام EMV در این زمینه نموده‌اند. هدف اصلی از ارایه این استاندارد، امکان بکارگیری یک کارت در تمام نقاط جهان می‌باشد.

کارت تراشه‌های شناخته شده در سطح جهان که با استاندارد EMV پیاده‌سازی شده اند عبارتند از:

- VIS – Visa
- M/Chip – MasterCard
- AEIPS – American Express
- CUP – China UnionPay
- J Smart – JCB
- D-PAS – Discover/Diners Club International

Visa و MasterCard این استاندارد را برای تراکنش‌های غیرحضوری از طریق تلفن و اینترنت نیز توسعه داده‌اند. MasterCard برای تجارت الکترونیک، برنامه احرازهویت تراشه (CAP[1]) به نام EMV-CAP و Visa طرح احرازهویت رمزعبور پویا (DPA[2]) را پیاده سازی نموده‌اند.

۳) مزایای EMV

EMV به طور قابل توجهی امنیت پرداخت کارت‌های مصرف‌کننده را از طریق کاهش پرداخت‌های جعلی (تقلبی و سرقت رفته) بهبود می‌بخشد.

ویژگی‌های EMV به شرح ذیل می‌باشد:

[1] Chip Authentication Program
[2] Dynamic Passcode Authentication

- احراز هویت کارت تراشه که به منظور بررسی واقعی بودن در تراکنش‌های آنلاین و آفلاین.
- پارامترهای مدیریت ریسک جهت تعیین شرایط برای صادرکننده کارت تراشه و همچنین الزام تراکنش‌ها جهت انجام عمل مجوزدهی تحت شرایط خاص در حالت آنلاین وآفلاین.
- امضای دیجیتالی اطلاعات پرداخت برای یکپارچگی معامله.
- تأیید قوی دارنده کارت برای محافظت در برابر تقلب.

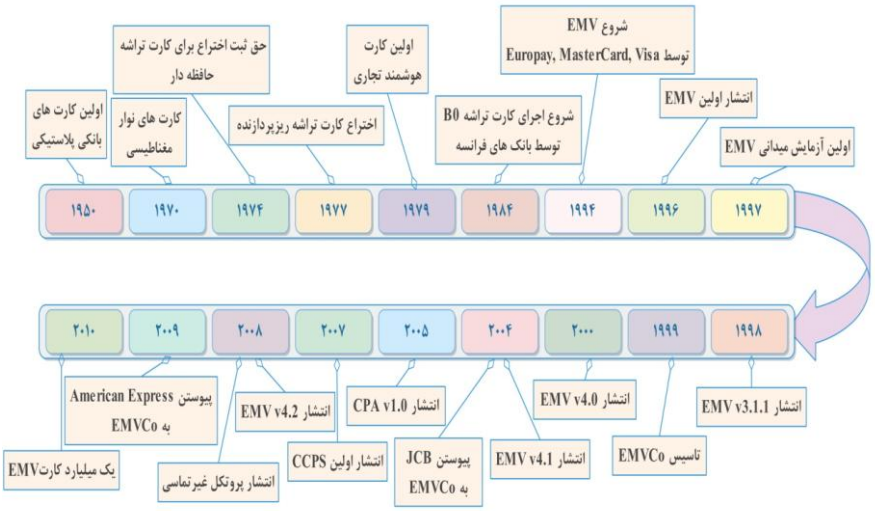
٤) تاریخچه EMV

سیر زمانی

اولین استاندارد برای کارت‌های پرداخت هوشمند Carte Bancaire M4 از Bull-CP8 در فرانسه در سال ۱۹۸۶ و به دنبال آن B4B0 در سال ۱۹۸۹ تدوین شد. در آلمان استانداردی به نام Geldkarte مطرح گردید.

استاندارد EMV در ابتدا در سال ۱۹۹۴ و ۱۹۹۳ نوشته شد. JCB در فوریه سال ۲۰۰۹ کنسرسیوم FI، China UnionPay در ماه مه ۲۰۱۳ و Discover در سپتامبر ۲۰۱۳ به کنسرسیوم پیوستند.

نسخه اولیه EMV در سال ۱۹۹۵ با عنوان EMV 2.0 انتشار پیدا کرد و در سال ۱۹۹۶ به EMV 3.0 و در سال ۱۹۹۸ به EMV 3.1.1 ارتقاء یافت. در سال ۲۰۰۰ نسخه 4 آن و به دنبال آن نسخه‌های 4.0، 4.1، 4.2 و 4.3 در سال‌های ۲۰۰۴، ۲۰۰۷، ۲۰۰۸ و ۲۰۱۱ منتشر گردید. در حال حاضر این استاندارد توسط EMVCo تعریف و مدیریت می شود و گواهی سازگاری با این استاندارد توسط این شرکت بعد از بررسی نتایج بررسی‌های انجام شده توسط یك آزمایشگاه معتبر، صادر می شود. بعد از پذیرفته شدن در آزمایش‌های مشترك EMVCo، نرم‌افزار باید برای سازگاری با EMV بررسی شود.



شکل ۶-۱: سیر زمانی EMV

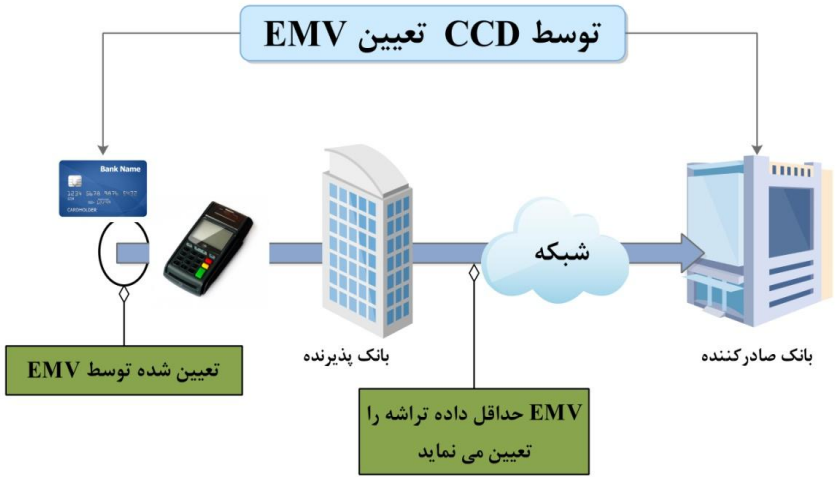
فهرست مستندات و استانداردهای EMV

پس از نسخه ۴، تمامی مشخصات کارت مدار مجتمع (ICC) سیستم پرداخت EMV در قالب چهار کتاب و چندین مستند دیگر منتشر گردید:

EMV Integrated Circuit Card Specifications for Payment Systems:

- Book 1 – Application Independent ICC to Terminal Interface Requirements
- Book 2 – Security and Key Management امنیت و مدیریت کلید
- Book 3 – Application Specification مشخصات برنامه‌های کاربردی
- Book 4 – Cardholder, Attendant, and Acquirer Interface Requirements الزامات رابط دارنده کارت، ارائه‌دهنده سرویس و پذیرنده
- Common Payment Application Specification
  مشخصات برنامه کاربردی پرداخت
- EMV Card Personalisation Specification
  مشخصات شخصی‌سازی کارت

در سال ۲۰۰۴، Common Core Definition (CCD) به عنوان بخشی از مشخصات EMV در نسخه 4.1 معرفی شد. CCD مجموعه ای از آپشن‌های پیاده سازی نرم‌افزار کارت، رفتار نرم‌افزار کارت، و تعاریف عنصر داده را جهت اجرای تراکنش EMV تعریف می‌کند. در صورت انطباق صادر کننده با CCD، یک نرم‌افزار مبتنی بر پرداخت تراشه EMV مشترک تعریف می‌شود که در تمام سیستم‌های پرداخت استفاده می‌گردد.



شکل ۶-۲: CCD

در سال ۲۰۰۵، EMVCo مشخصات کاربردی برای یک برنامه پرداخت صادرکننده با نام مشخصات کارت مدار مجتمع EMV برای برنامه پرداخت مشترک (CPA[1]) سیستم‌های پرداخت، که با الزامات CCD مطابقت دارد، و برنامه‌های کاربردی کارت، آپشن‌های پیاده‌سازی و رفتارهای نرم‌افزار کارت را تعریف می‌کند. صادرکنندگان می‌توانند کارت‌های تراشه مطابق با CPA را به عنوان جایگزین کارت تراشه انتخاب کنند که با مشخصات نرم‌افزار پرداخت کارت EMV سیستم پرداخت بین‌المللی مربوطه مطابقت داشته باشد.

[1] Common Payment Application

در سال ۲۰۰۷، مشخصات پروتکل ارتباط غیرتماسی EMV (CCPS[1]) منتشر شد به طوری که مشخصات سخت افزار و firmware (غیرتماسی سطح ۱) برای همه برنامه‌های کاربردی پرداخت سیستم پرداخت غیرتماسی مشترک خواهد بود.

شکل ۶-۳: NFC و غیرتماسی

مشخصات نقطه ورود[2] جهت تسهیل برنامه‌های کاربردی متعدد غیرتماسی سیستم پرداخت در یک ریدر غیرتماسی در سال ۲۰۰۸ منتشر گردید.

علاوه بر پذیرش کارت‌های تراشه غیرتماسی EMV، ریدرهای غیرتماسی منطبق بر مشخصات EMV می‌تواند طوری طراحی شود که تراشه‌های غیرتماسی تعبیه شده در سایر موارد مانند تلفن‌های همراه را نیز پذیرا باشد. که با پیاده‌سازی ارتباط حوزه نزدیک (NFC[3]) در تلفن همراه یا دستگاه معادل امکان‌پذیر است.

[1] Contactless Communication Protocol Specification
[2] Entry Point Specification
[3] Near Field Communication

EMV در دنیا

از شروع EMV در سال ۱۹۹۷، تا پیشرفت مهاجرت ملی از نوار مغناطیسی به تراشه EMV در بازارهای مختلف سراسر جهان، EMV یک استاندارد جهانی برای پرداخت تراشه گردید و استفاده از آن همچنان رو به رشد می‌باشد.

براساس آمار سال ۲۰۱۰، ۳۶ درصد از کل کارت، و ۶۵ درصد از کل پایانه‌ها مبتنی بر استاندارد EMV هستند. و ضریب نفوذ آن به تفکیک منطقه‌ای طبق آمار مذکور به شرح ذیل می‌باشد:

جدول ۶-۱: ضریب نفوذ EMV به تفکیک مناطق

منطقه	کارت	پایانه
کانادا، آمریکای لاتین، کارائیب	۲۶/۴	۵۵/۶
آسیا و اقیانوسیه	۲۶/۶	۴۱/۶
آفریقا و خاورمیانه	۱۳/۷	۶۲/۵
اروپا منطقه ۱	۶۵/۴	۸۴/۷
اروپا منطقه ۲	۱۱/۵	۶۱/۲
ایالات متحده	آمار در دسترس نمی‌باشد.	

۵) تفاوت EMVCo و سیستم‌های پرداخت بین المللی

جدول ۶-۲: تفاوت EMVCo و سیستم‌های پرداخت بین المللی

EMVCo	سیستم‌های پرداخت (MasterCard، Visa، American Express، JCB، ...)
- تصاحب و مدیریت مشخصات EMV - حفظ و توسعه بیشتر مشخصات EMV - مدیریت فرآیندهای تایید نوع برای پایانه - مدیریت فرآیند ارزیابی امنیت برای همه‌کارت‌های تراشه EMV - مدیریت فرآیند تایید نوع برای کارت‌های تراشه مطابق با CCD و CPA	- تعریف محصولات EMV - تعریف قوانین کسب و کار برای صدور و پذیرش محصولات EMV - تعریف پارامترها و ویژگی‌های EMV که بایستی مستقر شود - اجرای انطباق EMV - حفظ و انتشار مشخصات کارت سیستم پرداخت - پشتیبانی پیاده‌سازی EMV

٦) ارتباط EMVCo با سایر استانداردها:

مشخصات EMV نمی تواند به صورت ایزوله در نظر گرفته شود، و برای این منظور، EMVCo با دیگر نهادهای صنعت و سازمان‌های استانداردی به شرح زیر همکاری می‌کند:

International Organisation for Standardisation (ISO):

مشخصات EMV مبتنی بر استانداردهای سازمان بین‌المللی استانداردسازی (ISO) به شرح ذیل است:

- ISO/IEC 7816: Identification Cards – Integrated Circuit(s) Cards برای کارت‌های تماسی

  مشخصات EMV مبتنی بر سری استانداردهای ISO / IEC 7816 است. با این حال، اگر هر یک از مفاد و یا تعاریف خصوصیات EMV با سری استانداردهای ISO / IEC 7816 متفاوت باشد، مقررات EMV دارای اولویت خواهد بود.

- 7816-1 : مشخصات فیزیکی
- 7816-2 : کارت‌های تماسی – ابعاد و محل اتصال
- 7816-3 : پروتکل انتقال و رابط الکتریکی
- 7816-4 : سازمان، امنیت و دستورات تبادلی
- 7816-5 : نحوه ثبت کردن سازندگان برنامه‌های کاربردی
- 7816-6 : المان‌های داده‌های مبادله‌ای بین صنایع

➢ ISO/IEC 14443: Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards برای کارت‌های غیرتماسی

Payment Card Industry Security Standards Council (PCI SSC):

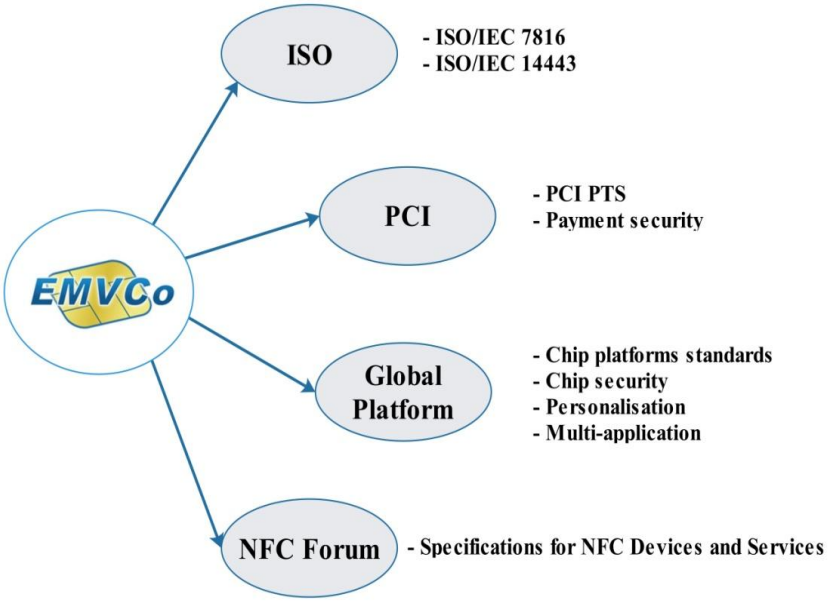
در درجه اول از اطلاعات حساس پرداخت مانند اطلاعات حساب و شماره شناسایی شخصی (PIN) حفاظت می‌کند. EMV و PCI در افزایش امنیت پرداخت و کاهش تقلب در کارت‌های جعلی و مفقودی و به سرقت مکمل می‌باشند. EMV قادر به حفاظت از اطلاعات کلیدی و جلوگیری از عناصر داده‌های تراکنش خاص نیست. بنابراین وجود استاندارد PCI DSS امری ضروری است.

The Near Field Communication (NFC) Forum:

بیشتر پرداخت‌های EMV از کانال‌های موبایل و غیرتماسی می‌باشد. بنابراین هماهنگی با NFC Forum جهت توسعه مشخصات اتصال میان دستگاه‌ها و خدمات NFC موردنیاز است.

GlobalPlatform:

بخشی از فعالیت‌های EMV بررسی عملکرد و امنیت پلتفرمی است که برنامه پرداخت EMV بر روی آن مستقر می‌شود. جهت حمایت از برنامه‌های متعدد، از منابع مختلف نیاز به هماهنگی با استانداردهای GlobalPlatform می‌باشد.

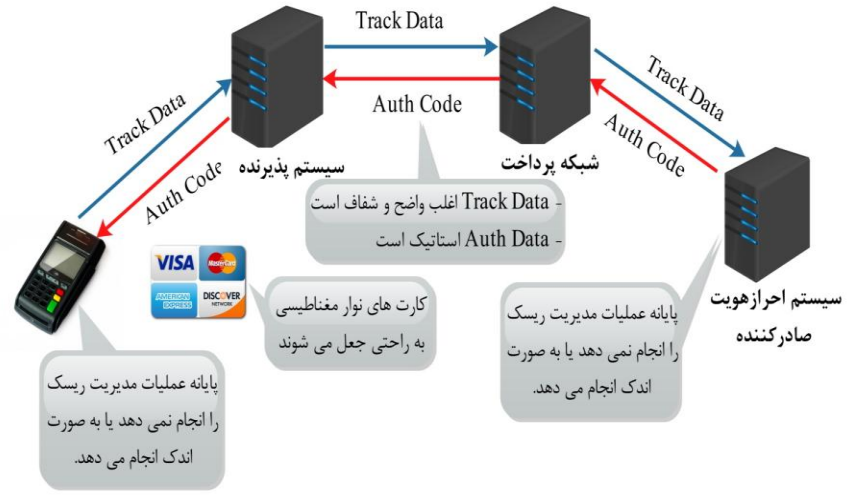


شکل ۶-۴: ارتباط EMVCo با سایر استانداردها

مراحل تراکنش و ویژگی‌های EMV

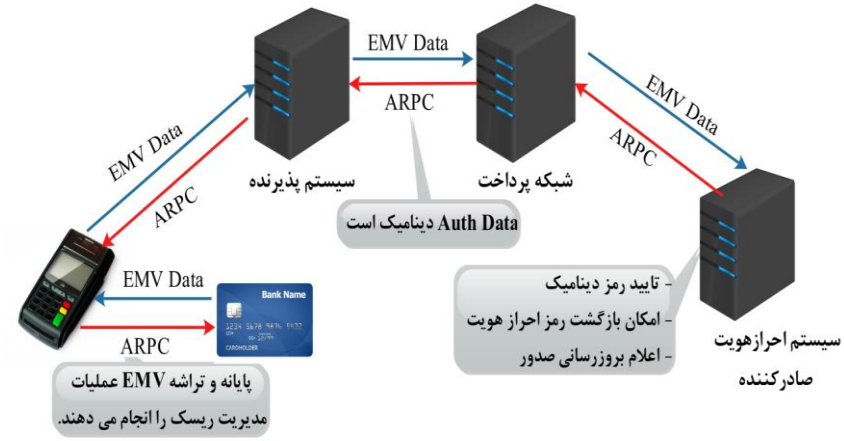
۱) تفاوت نوار مغناطیسی و تراشه

یک تفاوت اساسی میان تراکنش نوار مغناطیسی و تراشه EMV وجود دارد. در نوار مغناطیسی، کارت توسط پایانه خوانده شده و پایانه تمام مراحل پردازش را انجام و قوانین پرداخت را بکار می‌برد.



شکل ٦-٥: فرآیند تراکنش کارت مغناطیسی

در طول یک تراکنش EMV، تراشه قادر به پردازش اطلاعات و در واقع تعیین بسیاری از قوانین پرداخت است. پایانه به اجرای قوانین تعیین شده توسط صادرکننده در تراشه کمک می‌کند. این قوانین شامل اجرای خدماتی مانند احراز هویت داده آنلاین، تأیید هویت دارنده کارت از طریق PIN یا امضا، مجوز آنلاین و غیره است. بانک صادرکننده از طریق قوانین تراشه، سرویس مورد نیاز برای تراکنش را تعیین می‌نماید. در صورتی که پایانه قادر به ارائه سرویس مورد درخواست تراشه نباشد، در نتیجه‌ی رد تراکنش در تراشه، صادرکننده می‌تواند قوانین دیگری را تنظیم نماید.



شکل ۶-۶: فرآیند تراکنش کارت EMV

در یک تراکنش EMV نیاز به تعامل بین تراشه و پایانه است که مشخصاتEMV این پروتکل را تعریف می‌کند. این پروتکل دارای مراحلی به شرح ذیل می‌باشد:

مراحل تراکنش تماسی EMV

شکل ۶-۷: مراحل تراکنش تماسی EMV

انتخاب app: ممکن است بیش از یک نرم‌افزار EMV در تراشه وجود داشته باشد. پایانه و تراشه بر روی یک app رایج توافق نموده و برای استفاده در تراکنش انتخاب می‌کنند. اما در شرایط امکان انتخاب app توسط دارنده کارت از میان appهای پشتیبانی شده این مرحله اجرا می‌گردد.

آغاز پردازش app و قرائت داده app: app انتخاب شده آغاز و پایانه داده موردنیاز کارت تراشه را قرائت می‌کند.

احرازهویت داده آفلاین: از طریق SDA، DDA و یا CDA.

پردازش محدودیت‌ها: بررسی به منظور تشخیص اینکه تراشه مجاز به انجام تراکنش مورد درخواست می‌باشد.

تایید دارنده کارت: دارنده کارت از طریق یک روش پشتیبانی شده توسط پایانه تایید شده و توسط تراشه پذیرفته می‌شود. روش‌ها می‌تواند شامل امضا، PIN آنلاین، PIN آفلاین رمزشده، PIN آفلاین متنی، و یا بدون CVM باشد.

مدیریت ریسک پایانه: پایانه چندین بررسی انجام می‌دهد، مانند بررسی حد پایین جهت تعیین اینکه آیا نیاز برای پردازش آنلاین وجود دارد.

آنالیز اقدام پایانه: app پایانه بر اساس نتایج حاصل از احراز هویت داده آفلاین، محدودیت پردازش، تأیید دارنده کارت، مدیریت ریسک پایانه و قوانین پایانه و تراشه، درخواست یکی از نتایج رد آفلاین، تایید آفلاین یا آنلاین را می‌کند.

آنالیز اقدام کارت: بر اساس قوانین و محدودیت‌های صادرکننده، کارت با موارد زیر پاسخ خواهد داد: - ARQC آنلاین؛ - AAC: رد آفلاین؛ - TC: تایید آفلاین.

پردازش آنلاین: اگر تراشه درخواست آنلاین داشته باشد، پایانه یک درخواست آنلاین ایجاد و به میزبان صادرکننده برای مجوزدهی و احراز هویت کارت آنلاین ارسال می‌نماید. اگر پاسخ شامل احراز هویت صادرکننده انتخابی (ARPC) باشد، پایانه داده را به تراشه جهت تأیید ارسال می‌کند.

اتمام و پردازش اسکریپت: تراکنش تکمیل شد. اگر پردازش آنلاین رخ داده باشد تراشه درخواست پاسخ با TC (تایید) و یا AAC (رد) و اعمال هر گونه دستورات اسکریپت از طرف میزبان صادرکننده را خواهد کرد.

مراحل تراکنش غیرتماسی EMV

تفاوت عمده میان تراکنش تماسی EMV و تراکنش غیرتماسی EMV در سرعت انتقال اطلاعات بین تراشه و پایانه است که در غیرتماسی بالاتر بوده و برخی از مراحل تراکنش پس از نزدیکی و ترک تراشه انجام می‌گیرد (مجوزدهی آنلاین). هدف به حداقل رساندن مدت زمانی است که بایستی تراشه در مجاورت ریدر قرار گیرد.

۲) ویژگی‌های EMV

ویژگی‌های خاص تعریف شده توسط EMV در راستای دستیابی به حفاظت و کنترل به منظور کاهش تقلب در کارت‌های جعلی و مفقودی و سرقتی است:

رمز برنامه کاربردی

در طول یک تراکنش EMV، یک رمز برنامه کاربردی با استفاده از رمزنگاری two key triple DES تولید می‌شود. این رمز یک امضا است که از عناصر داده‌های مهم موجود در درخواست مجوز آنلاین به صادرکننده کارت (در صورت نیاز به مجوز آنلاین)، و یا در تراکنش نهایی مالی برای تسویه تولید می‌شود.

شکل ۶-۸: رمز برنامه کاربردی

رمزی که برای درخواست مجوز آنلاین تولید می‌شود رمز درخواست مجوزدهی (ARQC[1]) و رمزی که با امضای عناصر داده در زمان تایید پرداخت برای تسویه توسط تراشه تولید می‌شود گواهی تراکنش (TC[2]) نامیده می‌شود. اگر تراکنش رد شود، تراشه یک رمز به عنوان رمز احراز هویت برنامه کاربردی (AAC[3]) تولید می‌کند.

هدف از رمزهای برنامه کاربردی به دو قسم است:

- کارت آنلاین و احراز هویت صادرکننده

در زمانی که تراکنش پرداخت EMV آنلاین باشد، تراشه یک ARQC تولید می‌کند که در طی درخواست مجوز ارسال می‌شود. ARQC توسط میزبان صادرکننده تایید می‌نماید که تراشه تقلبی نمی باشد.

[1] Authorisation Request Cryptogram
[2] Transaction Certificate
[3] Application Authentication Cryptogram

به عنوان بخشی از فرایند مجوزدهی، ممکن است میزبان صادرکننده یک رمز بازگشتی به عنوان رمز پاسخ مجوزدهی (ARPC[1]) تولید کرده و به تراشه در پاسخ مجوز ارسال نماید. تایید صحت میزبان صادرکننده توسط تراشه با ARPC انجام می‌گیرد. بنابراین تمام محدودیت‌های آفلاین چیپ از بین می‌رود.

- امضای عناصر داده‌های تراکنش برای احراز هویت و تمامیت تراکنش

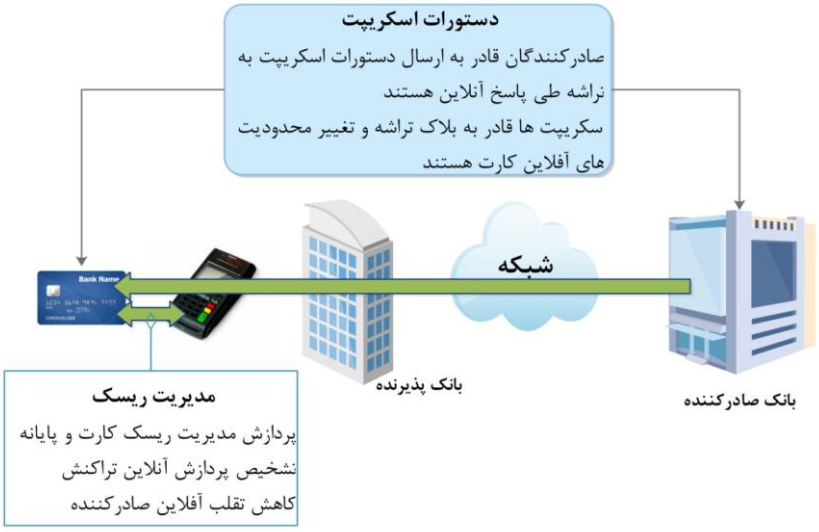
رمزهای ذیل توسط امضای عناصر داده‌های حیاتی در پیام تراکنش مربوطه تولید می‌شود. اعتبار این رمزها به گیرنده در تایید عناصر اطلاعات کمک می‌کند.

- ARQC - درخواست مجوز آنلاین؛
- ARPC - پاسخ مجوز آنلاین؛
- TC - پیام‌های مالی جهت تسویه تراکنش تاییدشده؛
- AAC – تراکنش رد شده.

مدیریت ریسک و کنترل مجوز

EMV امکان کنترل پایانه فروش را برای بانک صادرکننده جهت کاهش تقلب و ریسک اعتباری در تراکنش‌های آفلاین و کمتر از حد پایین فراهم می‌کند. بانک صادرکننده می‌تواند در کارت تراشه محدودیت تعداد تراکنش‌های آفلاین متوالی اعمال نماید.

[1] Authorisation Response Cryptogram



شکل ۶-۹: مدیریت ریسک و دستورات اسکریپتی

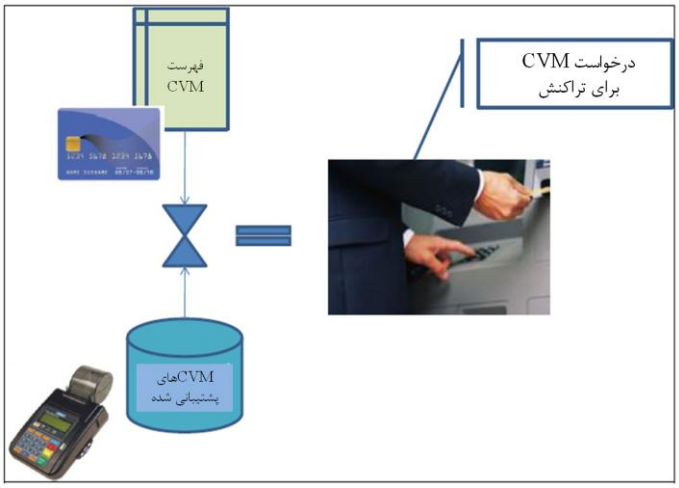
علاوه بر این، EMV دستورات اسکریپتی را جهت تغییر محدودیت‌های کارت توسط صادرکننده تعریف می‌نماید که می‌تواند در طی پاسخ مجوز آنلاین به کارت برگردد. صادرکنندگان امکان صدور اسکریپت برای جلوگیری و یا غیرفعال کردن یک کارت مفقودی یا سرقتی نیز دارند.

EMV، تحت کنترل پذیرنده وسیله‌ای برای پایانه‌های پذیرش جهت انتخاب تراکنش برای تایید آنلاین براساس حد پایین و همچنین معیارهای داخلی و یا خرده فروش و بکارگیری انتخاب تصادفی تراکنش کمتر از حد پایین جهت ارسال آنلاین فراهم می‌کند.

اقدامات مذکور در برابر استفاده از کارت‌های مفقودی یا سرقتی یا جعلی که برای تراکنش‌های کمتر از حد پایین استفاده می‌شود محافظت نموده و امکان مسدود نمودن دائم کارت سرقت رفته را برای صادرکننده فراهم می‌نماید.

پردازش تأیید دارنده کارت

در حمایت از تمام روش‌های موجود برای تأیید دارنده کارت نوار مغناطیسی، EMV دو ویژگی جدید تعریف می‌کند که انعطاف پذیری بیشتری در تعیین و اجرای روشهایی در طول پرداخت برای تایید دارنده کارت به عنوان صاحب واقعی کارت برای صادرکنندگان فراهم می‌نماید. این ویژگی به کاهش تقلب در کارت‌های مفقودی یا سرقتی کمک می‌کند.



شکل ۶-۱۰: پردازش تأیید دارنده کارت

ویژگی اول: فهرست روش تأیید دارنده کارت (CVM[1]) است که توسط صادرکننده در کارت تراشه تعریف شده است. فهرست CVM در شرایط پذیرش مختلف، روش تایید دارنده کارت را به ترتیب اولویت مشخص نموده و اگر توسط پایانه پشتیبانی شود، آنگاه به کاررفته و در غیر این صورت از روش‌های جایگزین استفاده می‌شود. برای مثال، در پایانه‌های پذیرش PIN (شاید در داخل کشور) از PIN و در هنگام سفر که PIN پشتیبانی نمی شود از امضا استفاده می‌نماید.

ویژگی دوم: یک CVM جدید از PIN آفلاین است. استفاده از PIN آفلاین کاملا اختیاری است، به طوری که امکان استفاده از یک کارت تراشه EMV به منظور تایید PIN

[1] Cardholder Verification Method

واردشده توسط دارنده کارت در PIN pad و سپس ارائه یک روش تأیید صحت دارنده کارت مبتنی بر PIN برای همه محیط‌های پذیرش تراکنش آنلاین و آفلاین، از جمله تراکنش‌های کمتر از حد پایین و آفلاین امکان پذیر است.

دو مشخصه PIN آفلاین تعریف شده توسط EMV وجود دارد:

- PIN آفلاین رمزشده که در آن از رمزنگاری کلید عمومی برای محافظت از PIN استفاده شده است که از ترمینال پذیرش به کارت برای تأیید ارسال می‌شود.
- PIN آفلاین متنی که PIN از ترمینال پذیرش به کارت برای تأیید به صورت واضح ارسال می‌شود.

احراز هویت داده آفلاین EMV

EMV یک ویژگی به عنوان احراز هویت داده آفلاین برای مبارزه با تقلب برای پرداخت کارت توصیف می‌کند که در پایانه‌های پذیرش کارت آفلاین انجام می‌شود. احراز هویت داده آفلاین برای احراز هویت داده پرداخت از رمزنگاری کلید عمومی بدون نیاز به ارتباط آنلاین با میزبان صادرکننده استفاده می‌نماید.

شکل ٦-١١: احراز هویت داده آفلاین

دو نوع احراز هویت داده آفلاین وجود دارد:

- احراز هویت داده استاتیک (SDA[1])
- احراز هویت داده دینامیک (DDA[2])، احراز هویت داده ترکیبی (CDA[3]) نوعی از DDA است.

در طول یک تراکنش پرداخت، کارت تراشه و پایانه استفاده از SDA، DDA و یا CDA را می‌پذیرند. تنها یک روش احراز هویت داده آفلاین برای یک تراکنش خاص به کار می‌رود. هنگامی که احراز هویت داده آفلاین انجام نشود، بایستی تراکنش EMV به صورت آنلاین مجوزدهی گردد.

تفاوت اساسی بین SDA و DDA این است که SDA خواندن داده برنامه پرداخت را از تراشه بدون دستکاری و یا تغییر نشان می‌دهد. SDA به این معنا نیست که کارت به صورت آفلاین احرازهویت شده است. زیرا امکان کپی کردن داده‌های کارت تراشه، از جمله رمز SDA، و ارسال آن را به کارت چیپ دیگری برای ایجاد یک کارت تقلبی که بتواند با موفقیت SDA را در پایانه فروش اجرا کند، وجود دارد. اما در DDA اطلاعات بر روی کارت از زمان صدور آن برای دارنده کارت قابل جایگزینی نبوده و کپی از کارت تراشه اصلی نیست. DDA، شکل قویتری از احراز هویت داده آفلاین نسبت به SDA است، زیرا DDA نشان می‌دهد که کارت به صورت آفلاین احراز هویت شده است.

CDA، به عنوان نوعی از DDA، برای مبارزه با حمله پیچیده در پایانه فروش طراحی شده است که مهاجم در پایانه فروش از یک کارت تراشه معتبر برای گذراندن احراز هویت داده آفلاین استفاده نموده، اما از آن پس در طول پرداخت، اقدامات کارت برای کسب مجوز را شبیه‌سازی می‌کند.

صادرکنندگان کارت یک روش احراز هویت داده آفلاین مبتنی بر عواملی مانند هزینه به ازای هر کارت و سرعت تراکنش را انتخاب می‌نمایند. این هزینه‌ها در برابر خطر حمله

[1] Static Data Authentication
[2] Dynamic Data Authentication
[3] Combined Data Authentication

کلاهبرداران کارت‌های تراشه با استفاده از روش‌های احراز هویت ضعیف تر مانند SDA سنجیده می‌شود، در حالی که هدف بسیار ساده تر ارائه شده توسط کارت‌های مغناطیسی هنوز رایج است.

اگر یک صادرکننده، کارت تراشه ای صادر کند که فقط مجاز به تراکنش‌هایی با مجوزدهی آنلاین باشد، تراشه به هیچ عنوان با احراز هویت داده آفلاین پشتیبانی نمی‌شود.

تست و تأییدیه EMV

۱) هدف کلیدی EMVCo

علاوه بر حفظ و تحول مشخصات EMV، نقش کلیدی و مکمل EMVCo، ارزیابی انطباق محصولات با مشخصات EMV، و تایید محصولات جهت عبور از آزمایش قبل از استقرار است.

فعالیت‌های متعدد که توسط EMVCo در حمایت از این هدف انجام می‌گیرد شامل تعریف و اجرای طرح تست براساس مشخصات EMV و تعریف و اجرای یک فرایند برای احراز صلاحیت ابزار تست است.

اجزای که شامل فرآیند تصویب EMV هستند به شرح ذیل می‌باشد:

۲) تایید نوع پایانه

تایید نوع پایانه توسط گروه کاری تصویب پایانه EMVCo (TAWG[1]) تعریف و اجرا شده و مطابقت پایانه‌های پذیرش EMV با الزامات کاربردی تعریف شده در مشخصات EMV ارزیابی می‌گردد. که شامل دو فرایند مجزا و مستقل می‌باشد.

- تایید نوع پایانه EMV سطح ۱ جهت بررسی مطابقت ریدر تراشه با مشخصات پروتکل مکانیکی و الکتریکی EMV سطح ۱ طراحی شده که انتقال داده‌ها بین پایانه و کارت را پوشش می‌دهد.

[1] Terminal approval Working Group

- تایید نوع پایانه EMV سطح ۲ جهت بررسی مطابقت عملکرد نرم‌افزار پایانه پذیرش با مشخصات EMV هسته EMV سطح ۲ طراحی شده است. قابلیت‌های نرم‌افزار غیر EMV که از توابعی مانند چاپگر و صفحه نمایش پشتیبانی کرده و پیام‌هایی برای ارسال به پذیرنده ایجاد می‌کند، بخشی از هسته در نظر گرفته نشده است.

۳) تایید نوع کارت

تایید نوع کارت توسط گروه کاری تصویب کارت EMVCo (CAWG[1]) تعریف و اجرا شده و مطابقت سخت افزار تراشه با مشخصات الکترومکانیکی و الزامات کاربردی تعریف شده در مشخصات EMV ارزیابی می‌گردد.

همچنین EMVCo فرایند تصویب نوع برنامه‌های کاربردی پرداخت تعبیه شده در تراشه را جهت مطابقت با Common Core Definition (CCD) و برنامه پرداخت مشترک (CPA) مدیریت می‌نماید.

٤) ارزیابی امنیت تراشه

ارزیابی امنیت تراشه EMVCo جهت ارزیابی تضمین تراشه برای حداقل سطح معینی از امنیت مورد نیاز برای پرداخت EMV طراحی شده و شامل مکانیزم‌ها و حفاظت امنیتی برای مقاومت در برابر حملات شناخته شده است. نتایج حاصل از ارزیابی امنیت تراشه EMVCo توسط هر یک از سیستم‌های پرداخت در فرآیند تایید کارت استفاده می‌شود.

ارزیابی امنیت عملکرد کارت جزو دامنه EMVCo نیست و توسط طرح‌های پرداخت اجرا می‌شود.

نکات پیاده‌سازی

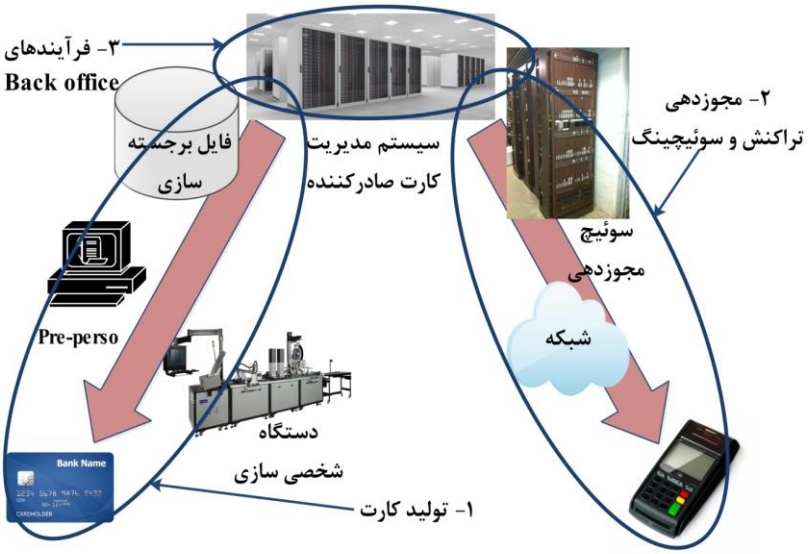
مهاجرت از نوار مغناطیسی به EMV نیازمند سرمایه گذاری در تغییر زیرساخت پرداخت و فرایندهای مرتبط است. تغییرات شامل پایانه‌های پذیرش نصب شده در

[1] Card Approval Working Group

خرده‌فروشی‌ها، سوئیچ و شبکه پذیرنده و سیستم میزبان مجوزدهی و تولید کارت صادرکننده می‌باشد. پیاده‌سازی و اجرای زیرساخت تراشه نقش EMVCo نیست بلکه وظیفه سیستم‌های پرداخت بین‌المللی و داخلی، صادرکنندگان کارت و پذیرندگان کارت می‌باشد.

۱) نکات صادرکنندگی

یک صادرکننده کارت تراشه EMV نیاز به در نظر گرفتن حداقل سه حوزه اصلی فعالیت پیاده‌سازی طبق نمودار زیر دارد:



شکل ۶-۱۲: فعالیت‌های پیاده سازی EMV صادرکننده

فعالیت‌های مذکور با جزئیات بیشتر در جدول زیر توضیح داده شده است:

جدول ۶-۳: فعالیت‌های صادرکنندگی EMV

فعالیت	توضیح
ارتقا فرآیند و زیرساخت تولید کارت و شخصی سازی آن برای تراشه.	انتخاب یک پلت فرم کارت تراشه با سخت افزار لازم است که مطابق با الزامات مورد نیاز برای صدور کارت‌های تراشه باشد. این الزامات شامل موارد ذیل است: ➢ نرم‌افزار واحد و یا چند نرم‌افزاری ➢ فقط پرداخت و یا پرداخت به همراه برنامه‌های کاربردی دیگر ➢ فقط تماسی و یا رابط دوگانه ➢ پشتیبانی از پردازش رمزنگاری مانند کلید عمومی.
	تعیین پارامترها و قوانین موردنیاز برنامه پرداخت تراشه که صادرکننده کارت برای کاهش تقلب در کارت‌های جعلی، مفقودی و سرقت رفته بایستی رعایت نماید.
	تولید کلیدهای رمزنگاری EMV مورد نیاز برای پشتیبانی از ویژگی‌های نرم‌افزار صادرکننده کارت برای کاهش تقلب در کارت‌های جعلی، مفقودی و سرقت رفته تقلبی.
	ارتقاء سیستم‌های تولید کارت فعلی از فرایند تحویل نوار مغناطیسی موجود به توانایی تولید و تحویل کارت‌های تراشه EMV.
ارتقاء سیستم‌های مجوزدهی و تسویه برای تراشه.	پیام‌های مجوزدهی و تسویه ناشی از تراکنش‌های کارت تراشه در پایانه فروش، اطلاعات جدید تراشه را حمل می‌نمایند. تغییرات برای سیستم‌های صادرکننده جهت صدور، مدیریت، مجوزدهی و تسویه متعلق به کارت‌های تراشه EMV و پشتیبانی از فرآیندهای عملیاتی موردنیاز است تا بتواند از مزایای داده‌های تراشه پیشرفته مانند سرویس مشتری، استردادوجه و اختلافات، تقلب، مدیریت ریسک اعتبار، و گزارش مدیریتی استفاده نماید.

فعالیت	توضیح
مهندسی مجدد فرآیندهای داخلی جهت پشتیبانی از تراشه.	بروزرسانی سرویس مشتری صادرکننده و عملیات Back Office. که شامل بروزرسانی فرآیندهای سرویس مشتری جهت پشتیبانی از کارت‌های تراشه EMV دارندگان کارت است. ابزاری لازم است تا اطلاعات لازم جهت رسیدگی به queryهای دارندگان کارت تراشه EMV در اختیار سرویس مشتری قرار گیرد. سیستم‌ها و فرآیندهایی لازم است تا عملیات Back Office کارت تراشه از جمله استردادوجه و اختلافات، بررسی تقلب و مدیریت ریسک اعتبار را پشتیبانی نماید.

۲) نکات پذیرندگی و خرده فروشی

یک پذیرنده و یا خرده فروش کارت تراشه EMV نیاز به در نظر گرفتن حداقل سه حوزه اصلی فعالیت پیاده سازی طبق نمودار زیر دارد:

شکل ٦-۱۳: فعالیت‌های پیاده سازی EMV پذیرنده

فعالیت‌های مذکور با جزئیات بیشتر در جدول زیر توضیح داده شده است:

جدول ۶-۴: فعالیت‌های پذیرندگی EMV

فعالیت	توضیح
استقرار پایانه پذیرش EMV، و آموزش مجدد اپراتورهای پایانه و ارتقاء خدمات پشتیبانی خرده فروش	خرید پایانه‌های تاییدشده پذیرش EMV. (پایانه‌هایی که پارامترهای EMV جهت پاسخگویی به الزامات پذیرش کارت‌های تراشه خرده فروش و پذیرنده در آنها نصب شده باشد و دارای تاییدیه EMV سطح ۱ و ۲ باشند.)
	بایستی نرم‌افزار پایانه‌های موجود با قابلیت EMV جدید که توسط هسته برنامه EMV سطح ۲ ارائه شده، یکپارچه گردد.
	ارتقاء سیستم‌های مدیریت پایانه به طوری که تنظیمات و پارامترهای EMV به صورت موثر و از راه دور اداره شود.
	استقرار پایانه‌ها در این زمینه. که شامل ارتقاء و یا تعویض سخت‌افزار ریدر تراشه و ارتقای نرم‌افزار به نرم‌افزار دارای قابلیت EMV مورد تایید EMVCo است.
	آموزش اپراتورها و صندوقداران پایانه‌ها جهت پذیرش کارت تراشه - وارد کردن کارت تراشه به جای کشیدن نوار مغناطیسی. علاوه بر این، آموزش کارکنان برای پیاده‌سازی و پشتیبانی تراشه.
ارتقا سیستم‌های میزبان جهت سوئیچ تراکنش‌های تراشه برای مجوزدهی و تسویه	ارتقا پایانه جهت رابط میزبان پذیرنده. (فرمت پیام برای رابط بین پایانه و خرده‌فروش و / یا میزبان پذیرنده نیاز به بروزرسانی جهت انتقال عناصر داده‌های تراشه EMV جدید می‌باشد.)
	ارتقا رابط‌های میزبان و تبادل.(پیام‌های خرده فروش و / یا میزبان پذیرنده که حاوی عناصر داده‌های EMV جدید از پایانه‌ها به لینک تبادل خروجی صادرکننده کارت می‌باشند، نیاز به بروزرسانی دارند.) این عمل نیازمند نگاشت عناصر داده‌ها از پیام‌های دریافتی بر روی لینک پایانه به پیام‌های خروجی بر روی لینک تبادل می‌باشد.

فعالیت	توضیح
مهندسی مجدد فرآیندهای داخلی جهت پشتیبانی از تراشه.	به روز رسانی عملیات Back Office و سرویس خرده فروشی به منظور استفاده از مزایای اطلاعات پیشرفته تراشه موجود در پیام تراکنش پایانه. که شامل روش‌های ارتقاء و عملیات کارکنان برای حمایت از عملکردهای زیر است: ➢ روش استرداد وجه و اختلاف تراکنش ➢ سرویس خرده فروش ➢ تشخیص تقلب

پیوست ۱

هر حمله دارای دو مرحله **شناسایی و بهره‌برداری** می‌باشد، و پتانسیل یک حمله بر اساس فاکتورهای زیر برای هر دو مرحله محاسبه می‌گردد:

- **زمان سپری‌شده:** زمان سپری‌شده بر حسب ساعت توسط فرد مهاجم برای شناسایی و یا بهره‌برداری یک حمله است.
  در محاسبه زمان از تساوی‌های ۱ روز = ۸ ساعت، ۱ هفته = ۴۰ ساعت، ۱ ماه = ۱۸۰ ساعت استفاده می‌شود.
- **تخصص و خبرگی:** تخصص به سطح دانش عمومی فرد مهاجم از حوزه برنامه کاربردی و یا نوع محصول (به عنوان مثال، سیستم عامل یونیکس، پروتکل اینترنت) اشاره دارد.
  چهار سطح تخصص در این خصوص تعریف شده است:
  - ناوارد: هیچ تخصص ویژه‌ای ندارد.
  - ماهر: آشنا به رفتار امنیتی محصول و حملات کلاسیک هستند.
  - متخصص: آشنا به الگوریتم‌ها، پروتکل‌ها، سخت‌افزار، سازه‌های اساسی اجراشده در محصول و یا نوع سیستم و اصول و مفاهیم امنیتی بکاررفته در آن و همچنین تکنیک‌ها و ابزار لازم برای تعریف حملات جدید هستند.
  - چندتخصصی: برای حملاتی که نیاز به زمینه‌های تخصصی کاملا متفاوت برای هر مرحله از حمله دارند.
- **دانش هدف ارزیابی (TOE):** میزان آشنایی از اطلاعات حساس و حیاتی طراحی محصول است، و به سه سطح به شرح زیر تقسیم می‌شود:
  - اطلاعات عمومی (و یا هیچ اطلاعاتی) در مورد TOE: اطلاعات عمومی که به راحتی توسط هر کسی به دست می‌آید (به عنوان مثال، از طریق اینترنت) و یا توسط فروشنده به هر مشتری ارائه می‌شود.
  - اطلاعات محدود (به عنوان مثال، از مشخصات فنی فروشنده به دست می‌آید): اطلاعات محدودی که بنا به درخواست توزیع و ثبت می‌شود، مثل مشخصات کاربردی.

- اطلاعات حساس (به عنوان مثال، دانش طراحی داخلی، که ممکن است از طریق مهندسی اجتماعی و یا مهندسی جامع معکوس کسب شود): مثال مناسب برای آن، اطلاعات طراحی سطح بالا (HLD[1]) و طراحی سطح پایین (LLD[2]) کد منبع (اصلی) است.

➢ **دسترسی به TOE:** دسترسی به TOE نیز یک فاکتور مهم است. فرض بر این است که TOE توسط فرد مهاجم خریداری شده، یا از طریق دیگری آن را به دست آورده است و هیچ محدودیت زمانی برای آنالیز و یا تغییر آن ندارد. بر اساس وضعیت و قابلیت‌های دستگاه تقسیم‌بندی می‌شود:

- نمونه مکانیکی یا غیرکاربردی: صرفا برای مطالعه طراحی مکانیکی و یا برای تامین قطعات یدکی استفاده می‌شود.
- نمونه کاربردی بدون کلید کار: برای رفتار منطقی و الکتریکی آن وسیله استفاده می‌شود اما با کلیدهای کار بارگذاری نشده و در نتیجه کاربردی در یک شبکه پرداخت یا کارت‌های پرداخت واقعی ندارند.
- نمونه کاربردی با کلید کار: دستگاه‌های کاملا کاربردی، که ممکن است برای بررسی روش حمله و یا انجام یک حمله مورد استفاده قرار گیرد.

➢ **تجهیزات:** اشاره به تجهیزاتی دارد که برای شناسایی و بهره برداری از آسیب‌پذیری لازم است. بر اساس قیمت و دردسترس‌پذیری تقسیم می‌شود:

- تجهیزات استاندارد: تجهیزاتی است که به راحتی برای شناسایی آسیب‌پذیری و یا حمله در دسترس مهاجم است. این تجهیزات می‌توانند به آسانی به دست آیند به عنوان مثال، از یک فروشگاه در نزدیکی و یا دانلود از اینترنت. این تجهیزات ممکن است از اسکریپت‌های ساده حمله، رایانه‌های شخصی، ریدرهای کارت، تولیدکننده مدل، میکروسکوپ نوری ساده، منبع برق، و یا ابزار مکانیکی ساده تشکیل شده باشد.
- تجهیزات تخصصی: به آسانی در دسترس مهاجم نیست، اما می‌تواند بدون تلاش زیاد به دست آید، که شامل خرید مقدار متوسط تجهیزات (به عنوان مثال،

[1] High-Level Design
[2] Low-Level Design

کارت‌های الکترونیکی اختصاصی، Test Benchهای تخصصی، آنالایزر پروتکل، اسیلوسکوپ، ایستگاه‌های کاری میکروپروب، میزکار شیمیایی، ماشین‌آلات دقیق فرز، و غیره) و یا توسعه اسکریپت و یا برنامه‌های حمله گسترده‌تر است.

- تجهیزات سفارشی: به آسانی در دسترس عموم نیست و نیاز به تولید خصوصی دارد (به عنوان مثال، نرم‌افزار بسیار پیچیده) یا تجهیزات خیلی تخصصی بوده و نیاز به کنترل توزیع و ایجاد محدودیت دارد. یا بسیار گران است (به عنوان مثال، پرتو یون متمرکز، میکروسکوپ الکترونی روبشی و تجهیزات لیزری ساینده).
- تجهیزات بسیار سفارشی: در مورد حملاتی است که نیاز به چند نوع از تجهیزات سفارشی برای مراحل مختلف حمله دارد.

➢ **قطعات:** قطعات موردنیاز برای مخفی‌کردن نشانه‌های یک حمله است؛ یا اجزایی که در طول یک حمله شکسته شده است، مانند یک بخش از Case، صفحه نمایش و یا یک چاپگر؛ یا قطعات موردنیاز برای ایجاد اشکالات مانیتورینگ داده و برقراری ارتباط؛ یا موردنیاز برای انجام یک حمله.

- قطعات استاندارد: به راحتی در دسترس مهاجم است، یا با خرید آنها از یک فروشگاه یا استفاده دوباره از قطعات یک نمونه مکانیکی همان دستگاه.
- قطعات تخصصی: به آسانی در دسترس مهاجم نیست اما می‌تواند بدون تلاش زیاد به دست آید.
- قطعات سفارشی: به آسانی در دسترس نیست و به طور خاص ساخته می‌شود. احتمال نیاز یک حمله به قطعات یدکی سفارشی بسیار کم است.

فاکتورهای فوق‌الذکر به شرح جدول ذیل امتیازدهی می‌شوند:

جدول پ-۱: امتیاز فاکتورهای محاسبه پتانسیل حمله

فاکتور	شناسایی	بهره‌برداری
زمان سپری‌شده		
کمتر از یک ساعت	۰	۰
کمتر از یک روز	۱	۲
کمتر از یک هفته	۲	۳
کمتر از یک ماه	۳	۴
بیشتر از یک ماه	۵	۷
تخصص و خبرگی		
شخص ناوارد	۰	۰
ماهر	۱	۱
متخصص و خبره	۲	۳
چندتخصصی	۵	۶
دانش هدف ارزیابی (TOE)		
عمومی	۰	۰
محدود	۲	۲
حساس	۳	۴
دسترسی به TOE*		
نمونه مکانیکی	۱	۱
نمونه کاربردی بدون کلید کار	۲	۲
نمونه کاربردی با کلید و نرم‌افزار کار	۴	۴
تجهیزات		
هیچ	۰	۰
استاندارد	۱	۲
تخصصی	۳	۴

فاکتور	شناسایی	بهره‌برداری
سفارشی	۵	۶
بسیار سفارشی	۷	۸
قطعات		
هیچ	۰	۰
استاندارد	۱	۱
تخصصی	۲	۲
سفارشی	۴	۴

* در صورت نیاز به بیش از یک دستگاه، مقادیر جدول بایستی در اعداد زیر ضرب شود:

جدول پ-۲: ضرایب دسترسی به TOE

ضرایب	تعداد دستگاه‌ها
۱	۱
۱/۵	۲
۲	۳-٤
٤	۵-۱۰
۵	بیشتر از ۱۰

منابع

1. Payment Card Industry (PCI) Data Security Standard (DSS), Requirements and Security Assessment Procedures, Version 3.1, April 2015, PCI SSC

2. Payment Card Industry (PCI) Data Security Standard (DSS), Quick Reference Guide, Understanding the Payment Card Industry, Version 3.1, May 2015, PCI SSC

3. Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS), Requirements and Security Assessment Procedures, Version 3.1, May 2015, PCI SSC

4. Payment Card Industry (PCI) Payment Application Data Security Standard (PA-DSS), Program Guide, Version 3.1, July 2015, PCI SSC

5. Payment Card Industry (PCI) PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements, Version 4.1c, November 2015, PCI SSC

6. Payment Card Industry (PCI) PIN Transaction Security (PTS) Hardware Security Module (HSM), Security Requirements, Version 2.0, May 2012, PCI SSC

7. Payment Card Industry (PCI) PIN Security, Requirements and Testing Procedures, Version 2.0, December 2014, PCI SSC

8. Payment Card Industry (PCI) PIN Security Requirements, Version 2.0, December 2014, PCI SSC

9. Payment Card Industry (PCI) Point-to-Point Encryption (P2PE), Solution Requirements and Testing Procedures, Version 2.0 (Revision 1.1), July 2015, PCI SSC

10. EMV Integrated Circuit Card Specifications for Payment Systems, Book 1 Application Independent ICC to Terminal Interface Requirements, Version 4.2, June 2008, EMVCo

11. EMV Integrated Circuit Card Specifications for Payment Systems, Book 2 Security and Key Management, Version 4.2, June 2008, EMVCo

12. EMV Integrated Circuit Card Specifications for Payment Systems, Book 3 Application Specification, Version 4.2, June 2008, EMVCo

13. EMV Integrated Circuit Card Specifications for Payment Systems, Book 4 Cardholder, Attendant, and Acquirer Interface Requirements, Version 4.2, June 2008, EMVCo

14. A Guide to EMV, V 1.0, May 2011, EMVCo

15. Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure, February 2011, Smart Card Alliance Payments Council

16. First Data's Program on EMV, November 2014, First Data

۱۷. چارچوب راهبرد راهبری و مدیریت کارت هوشمند در شبکه بانکی کشور، ۱۵/۱/۱۳۸۴، بانك مرکزی جمهوری اسلامی ایران، اداره نظام های پرداخت.