پیش نیازهای فنی مورد نیاز جهت اتصال شبکه‌های ملی پرداخت به شبکه‌های بین المللی

تهیه کنندگان:

ثنا کمرئی

مهتاب عرفاتی

از

مدیریت ریسک و امنیت اطلاعات شرکت خدمات انفورماتیک

تاریخ تهیه: 95/08/17

بدیهی است در شرایط پساتحریم، اتصال بانک‌ها و سوئیچ ملی کشور به شبکه‌های بین‌المللی یکی از موضوعات مهم در صنعت بانکداری است. در این حوزه سه مقوله "امنیت"، "کیفیت" و "انطباق با استانداردهای بین المللی" اهمیت پیدا خواهد کرد. در حال حاضر یکی از چالش‌های صنعت بانکداری، تطبیق این صنعت با استانداردهای اجرایی و فنی است که در حال حاضر در دنیا استفاده می‌شود. لازم است زیرساخت‌های بانکی کشور جهت اخذ مجوز برای عضویت در شرکت‌هایی مانند ویزا[1]، مسترکارت[2] و غیره با استانداردهای مشخص شده از سوی این شرکت‌ها هماهنگ شود. در ادامه با توجه به بررسی‌های انجام شده در سایت این شرکت‌ها و مستندات موجود در این سایت‌ها، قدم اول برای همکاری، پیاده‌سازی استانداردهای PCIDSS، PA-DSS ، PCI-PTS وEMV است که در بخش‌های بعدی با ذکر جزئیات آمده است.

1-شرایط فنی مورد نیاز برای همکاری با شرکت مسترکارت

با توجه به مستند MasterCard Rules که در سال 2014 توسط شرکت مسترکارت تدوین شده است، لازم است نام کشور درخواست کننده برای همکاری با این شرکت در جدولی که براساس مناطق جغرافیایی است وجود داشته باشد. این شرط به عنوان اولین الزام برای همکاری است. در قسمت دیگری از این مستند برای منطقه آسیا، پیاده‌سازی استاندارد EMV بصورت جداگانه قید شده است. همچنین انطباق با الزامات استاندارد PCI Security برای شرکت‌های ارائه دهنده سرویس الزامی است. در مستند Security Rules and Procedures که در سال 2015 تدوین شده، جزئیات بیشتری در رابطه با انطباق با الزامات این استاندارد آمده است.

براساس این مستند، تمامی شرکت‌های ارائه‌دهنده سرویس‌های بانکی[3] و فروشنده‌ها[4] لازم است الزامات استاندارد PCIDSS[5] را با رعایت موارد زیر پیاده‌سازی نمایند: (لازم به ذکر است که شرکت‌های ارائه‌دهنده سرویس‌های بانکی و فروشنده‌ها براساس ویژگی‌هایشان، سطح بندی می‌شوند.)

1- پس از تعیین دامنه مورد نظر، لازم است کلیه الزامات استاندارد PCIDSS برای این دامنه پیاده‌سازی شده و در فواصل زمانی تعیین شده بازبینی گردد. این بازبینی برای سطح 1 فروشنده‌ها و سطح 1 شرکت‌های ارائه‌دهنده سرویس‌های بانکی باید به صورت سالیانه انجام شود. فروشنده‌ها ، می‌توانند برای ارزیابی از ممیز داخلی و یا ممیز مستقل (خارجی) تایید شده توسط شرکت مسترکارت استفاده نمایند. شرکت‌های ارائه‌دهنده سرویس‌های بانکی باید برای ارزیابی از ممیز شخص ثالث تایید شده در سایت SDP Program[6] استفاده نمایند. تمامی این ارزیابی‌ها باید براساس روال ممیزی PCIDSS انجام گیرد. (نمونه ای از این روال ممیزی منطبق با استاندارد PCIDSS توسط این شرکت منتشر شده است.)

2- شرکت‌های ارائه‌دهنده سرویس‌های بانکی و فروشنده‌ها لازم است ممیزی داخلی انجام دهند و کلیه این ممیزی‌ها می‌تواند براساس مستند The Payment Card Industry Self-assessment Questionnaire که به صورت رایگان در

[1] Visa
[2] MasterCard
[3] Service Providers
[4] Merchant
[5] Payment Card Industry (PCI) Data Security Standard
[6] The MasterCard Site Data Protection (SDP) Program

سایت PCISSC وجود دارد انجام گیرد. سطح 2،3 و 4 فروشنده‌ها و سطح 2 شرکت‌های ارائه‌دهنده سرویس‌های بانکی باید سالانه سطح قابل قبولی را کسب نمایند.

3- تمامی شرکت‌های ارائه‌دهنده سرویس‌های بانکی و سطوح 1 تا 3 فروشنده‌ها لازم است اسکن آسیب پذیری‌های شبکه را در بازه‌های زمانی 3 ماهه انجام دهند. برای این منظور لیستی شامل نام کلیه شرکت‌های مورد قبول PCI که انجام دهنده‌ی این فعالیت هستند به نام Approved Scanning Vendors (ASVs) در سایت PCISSC وجود دارد. شرکت‌های ارائه‌دهنده سرویس‌های بانکی و فروشنده‌ها باید از این لیست استفاده نمایند. تمامی این اسکن‌ها می‌بایست براساس روال اسکن PCIDSS انجام گیرد. (نمونه‌ای از این روال درسایت PCI[7] وجود دارد.)

لازم است الزامات استاندارد PA-DSS توسط شرکت‌های شخص ثالث که توسعه دهنده برنامه‌های کاربردی برای شرکت‌های ارائه‌دهنده سرویس‌های بانکی و سطوح 1 تا 3 فروشنده‌ها هستند، نیز رعایت شود. مستنداتی در این رابطه تحت عنوان Payment Application Data Security Standard (PA-DSS) و PCI PA-DSS Program Guide بصورت رایگان در سایت PCISSC وجود دارد. همچنین برای این منظور لیستی شامل نام تمامی شرکت‌های مورد قبول PCI جهت ارزیابی و ممیزی در این زمینه در سایت PCISSC وجود دارد.

همان طور که در بالا ذکر شده است، شرکت‌های ارائه‌دهنده سرویس‌های بانکی و فروشنده‌ها با توجه به چندین معیار سطح بندی می‌شوند. بطورمثال شرکت‌های ارائه‌دهنده سرویس‌های بانکی سطح 1و2 باید الزامات زیر را دارا باشند.

سطوح ارائه دهندگان سرویس	الزامات
سطح 1 ارائه‌دهندگان سرویس	تمامی TPP[8] و DSE[9]هایی که سالیانه بیش از 300،000 تراکنش کارت‌ها Maestro و MasterCard را ذخیره، انتقال و پردازش می‌نمایند دارای سطح 1 هستند. - تمامی الزامات PCIDSS در دامنه تعیین شده پیاده‌سازی شود. - دامنه به صورت سالیانه توسط QSA[10]های مورد تائید PCI ممیزی شود. -اسکن آسیب پذیری‌های شبکه در بازه‌های زمانی 3 ماهه توسط ASVهای مورد تائید PCI انجام شود.
سطح 2 ارائه‌دهندگان سرویس	تمامی DSE هایی که سالیانه کمتر از 300،000 تراکنش کارت‌های Maestro و MasterCard را ذخیره، انتقال و پردازش می‌نمایند دارای سطح 2 هستند. - تمامی الزامات PCIDSS در دامنه تعیین شده پیاده‌سازی شود. - دامنه به صورت سالیانه با استفاده از پرسشنامه‌های PCI، ممیزی داخلی شود. - اسکن آسیب پذیری‌های شبکه در بازه‌های زمانی 3 ماهه توسط ASV های مورد تائید PCI انجام شود.

شرکت مسترکارت می‌تواند در صورت نیاز شرکت‌های ارائه‌دهنده سرویس‌های بانکی و فروشنده‌ها را براساس SDP Program ممیزی نماید.

[7] https://www.pcisecuritystandards.org

[8] Third Party Processor for example POI Terminal Operation, authorization routing, electronic data capture, clearing file preparation, submission, settlement, statement preparation and chargeback processing. In simpler terms, what we all know as an Acquiring Bank.

[9] Data Storage Entity for example a Web hosting company, payment gateway, terminal drivers and processors.

[10] Qualified Security Assessors

۲-شرایط فنی مورد نیاز برای همکاری با شرکت ویزا

با توجه به اطلاعات مندرج در سایت شرکت ویزا، موارد زیر به عنوان پیش نیاز برای همکاری با این شرکت آمده است:

1-انطباق با الزامات استاندارد PCIDSS برای تمامی شرکت‌های ارائه‌دهنده سرویس‌های بانکی و فروشنده‌ها الزامی است. (فایلی با نام Visa Introduces Enhanced PCIDSS Enforcement Plan توسط شرکت ویزا منتشر شده است که شامل برنامه‌ای برای پیاده‌سازی استاندارد PCIDSS، جهت استفاده برای شرکت‌هایی که به طور کامل این استاندارد را پیاده‌سازی نکرده‌اند، وجود دارد.)

2- شرکت‌های ارائه‌دهنده سرویس‌های بانکی، شرکت‌هایی هستند که اطلاعات کارت‌های ویزا را ذخیره، منتقل و پردازش می‌نمایند. شرکت ویزا این شرکت‌ها را براساس معیارهای مختلف سطح بندی می‌کند.

سطوح ارائه دهندگان سرویس	الزامات
سطح 1 ارائه دهندگان سرویس	تمامی VNP[11]ها و ارائه دهندگان سرویس‌های بانکی که سالیانه بیش از 300،000 تراکنش کارت‌های VISA را ذخیره، انتقال و پردازش می‌نمایند دارای سطح 1 هستند. - تمامی الزامات PCIDSS در دامنه تعیین شده پیاده‌سازی شود. -دامنه به صورت سالیانه توسط QSA های مورد تائید PCI ممیزی شود. -اسکن آسیب پذیری‌های شبکه در بازه‌های زمانی 3 ماهه توسط ASV های مورد تائید PCI انجام شود.
سطح 2 ارائه دهندگان سرویس	تمامی ارائه دهندگان سرویس‌های بانکی که سالیانه کمتر از 300،000 تراکنش کارت‌هایVISA را ذخیره، انتقال و پردازش می‌نمایند دارای سطح 2 هستند. - تمامی الزامات PCIDSS در دامنه تعیین شده پیاده‌سازی شود. - دامنه به صورت سالیانه با استفاده از پرسشنامه‌های PCI، ممیزی داخلی شود. -تمامی ارائه دهندگان سرویس‌های بانکی مستند AOC[12] موجود در سایت PCI را برای ممیزی داخلی تکمیل کرده و به شرکت ویزا ارائه نمایند. - اسکن آسیب پذیری‌های شبکه در بازه‌های زمانی 3 ماهه توسط ASVهای مورد تائید PCI انجام شود.

3-ارزیابی جهت انطباق با استاندارد PCIDSS به صورت سالیانه برای سطوح 1 و 2 شرکت‌های ارائه‌دهنده سرویس‌های بانکی الزامی است.

[11] VisaNet processors are entities that are directly connected to the Visa payment network and fulfill an essential role in the payment process and in protecting cardholder data.
[12] Attestation of Compliance

۳- سایر موارد

به دلیل حفظ امنیت و ارتقا آن در شبکه‌های بانکی کشور بهتر است قبل از اتصال به شبکه‌های بین المللی، به موارد زیر نیز توجه شود:

- پیاده‌سازی سیستم مدیریت تقلب و ضدپولشویی[۱۳]
- پیاده‌سازی الزامات استانداردهای ISO27001 سیستم مدیریت امنیت اطلاعات، ISO31000 مدیریت ریسک، ISO22301 مدیریت تداوم کسب و کار و ISO20000 مدیریت سرویس و اخذ گواهینامه‌های مرتبط با آن‌ها از شرکت‌های معتبر بین المللی مرجع صدور گواهینامه[۱۴]
- انجام برنامه‌ریزی‌هایی جهت مهاجرت به آخرین نسخه‌های استانداردهای بین المللی در صورتی‌که نسخه‌های قدیمی این استانداردهای در شبکه‌های بانکی، پیاده‌سازی شده باشد.
- ایجاد زیرساخت‌های ارزیابی و ممیزی امنیت سامانه‌ها و شبکه‌های بانکی

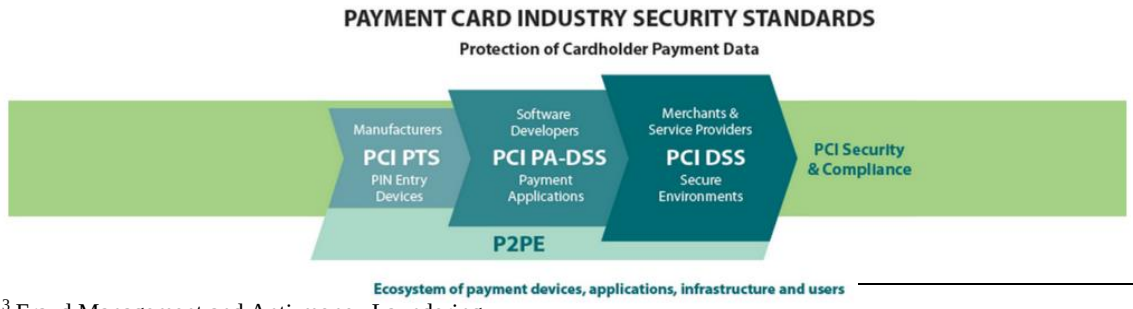
پیوست: تعریف الزامات مرتبط

- **استاندارد EMV**

کلمه EMV مخفف نام سه شرکت Europay، MasterCard وVisa است که این استاندارد را ایجاد کرده‌اند. در حال حاضر این استاندارد توسط .EMVCo مدیریت می‌شود. موضوع اصلی EMV، بحث احرازهویت ابزارپرداخت است، اینکه ابزار پرداخت واقعی باشد و جعل نشود. استاندارد EMV، استاندارد فنی کارت‌های پرداخت هوشمند و پایانه‌های پرداخت و دستگاه خودپرداز است. کارت‌های EMV، کارت‌های هوشمندی است که اطلاعات را بر روی تراشه به جای نوار مغناطیسی ذخیره می‌کند. بزرگ‌ترین تأثیر پیاده‌سازی این استاندارد ارتقا امنیت و کاهش تعداد برداشت‌های غیرمجاز از طریق روش‌هایی مانند تقلب است. برای افزایش قابلیت و ویژگی‌های امنیتی لازم است این استاندارد در هر دو قسمت کارت و پایانه پیاده‌سازی شود.

- **مجموعه استانداردهای PCI**

این استاندارد شامل الزامات امنیتی برای حفظ و نگهداری اطلاعات کارت است. کلیه سازمان‌هایی که اطلاعات کارت را ذخیره، پردازش و منتقل می‌نمایند ملزم به رعایت این استاندارد هستند. استاندارد PCI، راهنمایی جهت حفظ امنیت پرداخت است که شامل الزامات فنی و عملیاتی برای سازمان‌های پذیرنده و پردازش‌کننده تراکنش‌های پرداخت، توسعه‌دهندگان نرم‌افزاری و تولیدکنندگان برنامه‌های کاربردی و تجهیزات مورد استفاده در حوزه پرداخت است.



[13] Fraud Management and Anti-money Laundering
[14] Certificate Body

- استاندارد PCI-PTS

استاندارد PCI-PTS (PCI PIN Transaction Security Requirements) مجموعه‌ای از نیازمندی‌های ارزیابی است که توسط شورای استانداردهای امنیتی صنایع پرداخت کارت، برای پایانه‌های POI پذیرنده PIN ارائه شده است. این استاندارد بر روی مدیریت تجهیزات استفاده شده در حفاظت PINهای صاحبان کارت و سایر فعالیت‌های مرتبط با پردازش تراکنش‌ها است. تولیدکنندگان باید این الزامات را در مراحل طراحی و تولید در نظر بگیرند. این مجموعه نیازمندی‌هایی برای تمام پایانه‌هایی که رمز مشتری را دریافت می‌کنند، از جمله دستگاه‌های خودپرداز، پایانه‌های فروش، PIN Padها و غیره ارائه می‌دهد.

- استاندارد PA-DSS

استاندارد PA-DSS (Payment Application Data Security Standard) برای فروشندگان نرم‌افزار و توسعه دهندگان برنامه‌های پرداخت که اطلاعات صاحب کارت و یا داده‌های حساس احراز هویت را ذخیره، پردازش و انتقال می‌دهند، کاربردپذیر است. برای مثال هنگامی که این برنامه‌های کاربردی به افراد شخص ثالث فروخته می‌شوند و یا مجوز داده می‌شوند. اکثر شرکت‌های تولیدکننده کارت، فروشندگان را به استفاده از برنامه‌های کاربردی پرداخت که ارزیابی و تایید شده توسط کنسول PCI هستند، تشویق می‌نماید.

- استاندارد PCIDSS

استاندارد امنیت داده (DSS) صنایع پرداخت کارت (PCI) به منظور ترغیب و پیشبرد امنیت اطلاعات صاحبان کارت تدوین شده است. این استاندارد برای کلیه سازمان‌های مرتبط با پردازش کارت‌های پرداخت شامل فروشندگان، پردازش کننده‌ها، کارفرمایان، صادرکنندگان و ارائه دهندگان خدمات و سایر سازمان هایی که داده‌های صاحبان کارت را ذخیره، پردازش و انتقال می‌نمایند، کاربردپذیر است.

- **SDP Program**

به منظور انطباق با استاندارد PCI DSS شرکت مسترکارت برنامه(SDP (Site Data Protection Program را پیشنهاد داده است. در این مستند، الزامات استاندارد PCI DSS با جزئیات توضیح داده شده است.