مدیریت کل فناوری اطلاعات

اداره نظام‌های پرداخت

مقدمه‌ای بر پرداخت مبتنی بر نشان‌گذاری

نسخه اول

چهارم مرداد ماه هزار و سیصد و نود و شش

شناسنامه سند
نام سند: مقدمه‌ای بر پرداخت مبتنی بر نشان‌گذاری
نام تهیه‌کننده: بانک مرکزی جمهوری اسلامی ایران
طبقه‌بندی: حساس
تاریخ تهیه: ۱۳۹۶/۰۵/۰۴
نسخه: ۱,۰
تعداد صفحات: ۲۰
پیوست و ضمایم: دارد

کنترل نسخ مستندات			
نسخه	**موضوع بازنگری**	**تاریخ بازنگری**	**تهیه‌کننده**
-	-	-	-

فهرست مطالب

مقدمه ۶
۱- تعاریف ۸
۱-۱- نشانه و انواع آن ۸
۱-۱-۱- انواع نشانه براساس کاربرد ۸
۱-۱-۲- انواع نشانه براساس مدت اعتبار ۹
۱-۲- نشان‌گذاری ۱۰
۲- کاربرد نشان‌گذاری در شبکه پرداخت ۱۱
۳- فعالیت‌های اکوسیستم نشان‌گذاری ۱۳
۳-۱- درخواست‌دهنده نشانه ۱۳
۳-۲- سرویس‌دهنده نشانه ۱۶
پیوست یک- واژگان ۱۸
مراجع ۲۰

فهرست اشکال

شکل ۱- نشانه پرداخت ۸
شکل ۲- نشانه غیرپرداخت ۹
شکل ۳- کاربردهای نشان‌گذاری ۱۱
شکل ۴- درخواست‌دهندگان نشانه ۱۳
شکل ۵- نمونه کاربرد *Google Wallet* ۱۵
شکل ۶- نمونه کاربرد *Apple Pay* ۱۶

فهرست جداول

جدول ۱- واژگان ۱۸

مقدمه

در حال حاضر روند توسعه سیستم‌های پرداخت در راستای بهره برداری از ابزارها و فناوری‌های جدید به عنوان کانال پرداخت است. این در حالی است که افزایش تعداد کانال‌های پرداخت، موجب پیچیده‌تر شدن تامین امنیت و بوجود آمدن تهدیدات جدید در این حوزه شده و بانک‌ها در حین استفاده از فرصت پیش آمده، باید سازوکارهای جدیدی را نیز برای تامین امنیت بکارگیرند.

برای نمونه اگرچه استفاده از کارت‌های مبتنی بر *EMV* می‌تواند برای تراکنش‌های کارتی[1] امنیت مورد نیاز را تأمین نموده و امکان جعل کارت را کاهش دهد، اما بکارگیری این فناوری، کاهش تقلب‌های غیرکارتی[2] و امنیت محیط‌های نوظهور که از کانال‌های پرداخت گوناگون استفاده می‌کنند را پوشش نمی‌دهد. در چنین شرایطی سیستم‌های نشان‌گذاری[3] پرداخت، با جایگزین کردن شماره کارت با نشانه، قادرند این نیاز را پاسخ دهند.

در مدیریت ریسک، دو مقوله احتمال وقوع ریسک و شدت اثر وقوع ریسک اهمیت دارد. طبق نکات مطرح شده، سازوکارهای امنیتی مانند *EMV* احتمال وقوع ریسک را کاهش می‌دهد، در حالی که نشان‌گذاری به دنبال کاهش شدت اثر وقوع ریسک است. برای اینکه نشانه‌های پرداخت بتوانند امنیت مضاعفی در برابر سوءاستفاده‌های احتمالی تأمین کنند، لازم است در دامنه کاربرد خاصی تعریف شده و مورد استفاده قرار گیرند.

به صورت کلی استفاده از نشانه‌های پرداخت، برای تمامی ذی‌نفعان اکوسیستم پرداخت، مزایایی را در بردارد. صادرکنندگان کارت و دارندگان کارت می‌توانند از روش‌های پرداخت امن‌تر و کاهش ریسک تقلب بهره‌مند شوند. علاوه بر این با کاهش تهدیدهای حملات برخط و دزدی اطلاعات کارت، پذیرندگان و صاحبان کسب وکار نیز از سطوح اطمینان بالاتر در پرداخت بهره خواهند برد. همچنین شبکه‌های پرداخت قادر خواهند بود با کمترین تغییر در تعاملات فی‌مابین و کاهش نیازمندی‌های امنیتی در سطح شبکه فعالیت کنند.

علاوه بر مزایای مطرح شده، دلایل دیگری وجود دارد که بر اهمیت نشان‌گذاری افزوده است. با توجه به استاندارد امنیتی *PCI DSS*[4] بخش‌هایی از شبکه بانکی که به اطلاعات کارت دسترسی دارند دارای ریسک

[1] *Card-Present*

[2] *Card-Not-Present*

[3] *Tokenization*

[4] *Payment Card Industry Data Security Standard*

امنیتی بالایی نیز خواهند بود که با پیاده‌سازی پرداخت مبتنی بر نشانه و جایگزینی اطلاعات کارت با اطلاعات نشانه، دامنه استقرار استاندارد *PCI DSS* کاهش یافته و انطباق با آن آسان‌تر خواهد شد. همچنین با توجه به روند رو به رشد تکنولوژی‌ها، مانند *IOT* و گسترش فعالیت *FinTech* ها، می‌توان اظهار داشت که استفاده از سیستم نشان‌گذاری موجب تسهیل مسیر پیشرفت این‌گونه فعالیت‌ها همراه با کنترل ریسک‌های امنیتی مرتبط با اطلاعات کارت می‌شود.

با توجه به اهمیت موضوع پرداخت مبتنی بر نشان‌گذاری، مستند پیش‌رو به منظور معرفی این موضوع براساس به‌روش‌ها و چارچوب‌های تاییدشده بین‌المللی تهیه شده است.

۱- تعاریف

در این بخش از مستند تعاریف اولیه نشان‌گذاری مورد توجه قرار گرفته است.

۱-۱- نشانه[1] و انواع آن

عبارت نشانه به مقدار جایگزین شماره کارت گفته می‌شود که در ادامه انواع آن براساس کاربرد و مدت اعتبار تعریف شده است.

۱-۱-۱- انواع نشانه براساس کاربرد

طبق تعاریف ارائه شده در چارچوب فنی *EMVCo [1]* و راهنمای نشان‌گذاری *PCI DSS [2]* براساس کاربردهای نشانه، دو نوع نشانه پرداخت و نشانه غیرپرداخت وجود دارد.

نشانه پرداخت[2]:

- یک شماره ۱۳ تا ۱۹ رقمی با ساختاری مشابه شماره کارت
- قابلیت صدور و مسیردهی[3] تراکنش براساس این نوع نشانه
- لزوم استفاده از این نوع نشانه براساس چارچوب فنی *EMVCo*

در راهنمای موسسه گارتنر *[4]* به نشان‌گذاری براساس این نوع نشانه، نشان‌گذاری صادرکننده[4] گفته می شود که نمونه‌ای از آن در شکل ۱ مشاهده می شود. در این مستند منظور از نشانه، نشانه پرداخت می‌باشد.

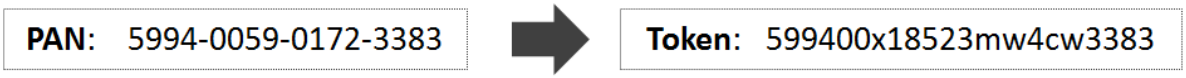
شکل ۱- نشانه پرداخت

[1] *Token*
[2] *Payment Token*
[3] *Routing*
[4] *Issuer Tokenization*

نشانه غیر پرداخت[1]:

- یک مقدار جایگزین برای شماره کارت با هدف ذخیره‌سازی آن به جای شماره کارت
- این نوع نشانه برای ذخیره‌سازی مورد استفاده قرار می‌گیرد.
- عدم امکان صدور یا مسیردهی تراکنش با استفاده از این نوع نشانه
- قابل استفاده برای انطباق با الزام استاندارد *PCI DSS* مبنی بر عدم ذخیره‌سازی شماره کارت به صورت خوانا

در راهنمای موسسه گارتنر *[5]* به نشان‌گذاری براساس این نوع نشانه، نشان‌گذاری پذیرنده[2] گفته می‌شود، که نمونه‌ای از آن در شکل ۲ مشاهده می‌شود.



شکل ۲- نشانه غیرپرداخت

۲-۱-۱- انواع نشانه براساس مدت اعتبار

طبق تعاریف ارائه شده در چارچوب فنی *EMVCo [1]* و راهنمای نشان‌گذاری *PCI DSS [2]* براساس مدت اعتبار، دو نوع نشانه *Multi-use* و *Single-use* وجود دارد.

- **نشانه *Multi-use***

اعتبار این نشانه براساس فاکتورهای مشخصی (تاریخ انقضا، تعداد تراکنش، سقف تراکنش و ...) تعیین می‌شود.

مزایا:

- ردیابی چندین تراکنش به کمک این نوع نشانه
- محدود نمودن پیام‌ها میان موجودیت‌های اکوسیستم نشان‌گذاری برای صدور نشانه‌ها

معایب:

- نیازمندی به درجه بالاتری از مکانیزم‌های امنیتی و سطوح ضمانت هنگام صدور این نوع نشانه

[1] *Non-Payment Token*

[2] *Merchant/Acquirer Tokenization*

- افزایش امکان ایجاد تراکنش تقلبی به دلیل معتبر بودن نشانه در چند تراکنش

- **نشانه *Single-use***

این نوع نشانه تنها برای یک تراکنش کاربرد دارد و پس از آن قابل استفاده جهت انجام تراکنش نخواهد بود. این نوع نشانه، معایب و مزایایی را شامل می‌شود که در ادامه به آن‌ها پرداخته شده است.

مزایا:

- افزایش سطح امنیت بنا بر صدور نشانه جدید برای هر تراکنش
- عدم نیازمندی ذخیره‌سازی نشانه سمت دارنده کارت

معایب:

- افزایش پیام‌ها میان موجودیت‌های اکوسیستم نشان‌گذاری برای صدور نشانه‌ها و تحت تاثیر قرارگرفتن کارایی سیستم‌ها
- پیچیده‌تر شدن تراکنش‌هایی مانند برگشت از خرید به دلیل عدم امکان استفاده از نشانه تراکنش اصلی
- در صورتی که قالب این نوع نشانه براساس چارچوب فنی *EMVCo* باشد، تعداد نشانه‌های قابل استفاده با محدودیت روبرو خواهد بود.

۲-۱- نشان‌گذاری

طبق تعریف ارائه شده در چارچوب فنی نشان‌گذاری *EMVCo [1]*، فرایندی که طی آن شماره کارت با نشانه، جایگزین شود را فرایند نشان‌گذاری می‌نامند. نشان‌گذاری ممکن است به منظور ارتقاء کارایی تراکنش، بهینه‌سازی امنیت تراکنش، یا ارائه روش جدیدی برای گسترش امکان فعالیت شرکت‌های ثالث (مانند شرکت‌های نوپایی که با ارائه خدمات از طریق پرداخت امن و سریع می‌توانند وارد بازار کار شوند) استفاده شود.

برای اینکه نشانه‌های پرداخت بتوانند امنیت مضاعفی در برابر سوءاستفاده‌های احتمالی تأمین کنند؛ نشانه پرداخت باید در دامنه خاصی مورد استفاده قرار گیرد؛ برای مثال می‌توان کاربرد نشانه را براساس کسب‌وکار، کانال پرداخت مشخص، موقعیت جغرافیایی، مبلغ تراکنش و تعداد تراکنش محدود کرد. این کنترل‌های محدودیت دامنه نشانه، مزیت کلیدی نشانه‌های پرداخت بوده و باید هر نشانه تنها در دامنه تعریف شده (کانال پرداخت، فروشنده بخصوص و ...) قابل استفاده باشد.

۲- کاربرد نشان‌گذاری در شبکه پرداخت

برخی از موارد کاربرد نشان‌گذاری در شبکه پرداخت در شکل ۳ نمایش داده شده است.

شکل ۳- کاربردهای نشان‌گذاری

به عنوان نمونه‌ای از پرداخت از طریق *NFC*، می‌توان به شرکت اپل اشاره نمود. این شرکت راهکار پرداخت موبایلی با عنوان *Apple-Pay* را که از سیستم نشان‌گذاری استفاده می‌کند در سال ۲۰۱۴ معرفی نمود. راهکار مذکور علاوه بر پرداخت از طریق *NFC*، امکان پرداخت درون‌برنامه‌ای[1] را نیز فراهم ساخته است. در روش پرداخت از طریق *NFC* زمانی‌که یک تراکنش آغاز می‌شود، دستگاه موبایل و/یا سرور راه دور، یک تراکنش مجاورتی را براساس اطلاعات مربوط به نشانه، تولید کرده و از طریق واسط *NFC* به ترمینال فروش ارسال می‌کند.

در کاربرد بارکد دوبعدی[2]، جهت آغاز تراکنش در ترمینال فروش، برنامه کاربردی داخل دستگاه موبایل یک بارکد دوبعدی پویا ایجاد می‌کند. زمانی‌که تراکنش آغاز می‌شود، دستگاه موبایل یک تراکنش شامل اطلاعات

[1] *In-App*
[2] *QR Code*

مربوط به نشانه پرداخت را تولید کرده و به ترمینال فروشنده ارسال می‌کند. همچنین این تراکنش می‌تواند با برقراری ارتباط با کیف پول دیجیتال نیز آغاز شود.

پرداخت اینترنتی به سناریوهایی اشاره دارد که در آن‌ها دارنده کارت، پرداخت را از طریق یک سایت فروشگاه اینترنتی با استفاده از کیف پول دیجیتال برای انتقال پرداخت و سایر اطلاعات سفارش انجام می‌دهد. زمانی‌که دارنده کارت در یک سایت اینترنتی که از کیف پول دیجیتال پشتیبانی می‌کند پرداخت را آغاز می‌کند، کیف پول دیجیتال از طریق واسط نرم‌افزاری[1] مربوطه، اطلاعات مربوط به نشانه پرداخت را به فروشنده ارسال می‌کند.

کاربرد پرداخت درون‌برنامه‌ای نیز به سناریوهایی اشاره دارد که در آن، داده کارت پرداخت از طریق برنامه کاربردی فروشنده دریافت و ذخیره می‌شود و به منظور برطرف کردن خطر امنیتی ذخیره داده کارت، نشانه پرداخت به جای شماره کارت نگهداری می‌شود.

[1] *API*

۳- فعالیت‌های اکوسیستم نشان‌گذاری

مطابق با چارچوب فنی *EMVCo [1]*، برای پیاده‌سازی راه‌حل نشان‌گذاری، لازم است فعالیت‌های جدیدی در اکوسیستم پرداخت تعریف شود که این فعالیت‌ها در دو بخش "درخواست‌دهنده نشانه[1]" و "سرویس‌دهنده نشانه[2]" قابل انجام است. در ادامه به بررسی فعالیت‌های مورد نیاز در این دو بخش پرداخته شده است.

۳-۱- درخواست‌دهنده نشانه

درخواست‌دهندگان نشانه لازم است در ابتدا توسط سرویس‌دهنده نشانه ثبت شده و با نیازمندی‌های ثبت‌نام، سیستم‌ها و فرایندهای مختص آن‌ها سازگار باشند. بعد از ثبت موفق، یک شناسه درخواست‌دهنده نشانه به آن‌ها اعطا خواهد شد. فعالیت‌کلیدی در نظر گرفته شده در این حوزه، ارائه درخواست نشانه از طرف دارنده کارت به سرویس دهنده نشانه جهت تبدیل شماره کارت به نشانه است.

درخواست‌دهندگان نشانه می‌توانند همان مشارکت‌کنندگان سنتی صنعت پرداخت یا مشارکت‌کنندگان نوظهور در این صنعت باشند. در شکل ۴ اعضای دارای قابلیت ایفای نقش درخواست‌دهنده نشانه با ذکر مثال نشان داده شده است *[3]*.

بانک صادرکننده	فروشگاه اینترنتی	ارائه‌دهنده خدمات پرداخت	سازنده تجهیز همراه	ارائه‌دهنده کیف پول دیجیتال
Card Issuers	E-commerce Merchants	Payment Processors and Payment Gateway Providers	Device Manufacturers	Digital Wallet Providers
Issuer Banks	Amazon	PSP	Samsung Pay	Google Wallet

شکل ۴- درخواست‌دهندگان نشانه

[1] *Token Requestor*

[2] *Token Service Provider*

ارائه‌دهندگان کیف پول دیجیتال به عنوان یکی از پرکاربردترین درخواســـت‌دهندگان نشـــانه در پرداخت همراه محسـوب می‌شـوند. کیف پول دیجیتال، برنامه کاربردی اسـت که اصـلی‌ترین هدف آن نگهداری اطلاعات مرتبط با کارت‌های م شتری به منظور ا ستفاده آ سان در هنگام خرید ا ست. در سی ستم ن شان‌گذاری به دلیل کاهش ریسک‌های امنیتی، اطلاعات نشانه به جای اطلاعات کارت ذخیره و نگهداری می‌شود. ذکر این نکته لازم است که در این نوع پرداخت، تراکنش از کیف پول دیجیتال آغاز می‌شود و اطلاعات مربوط به نشانه را به پلتفرم سمت فروشنده ارسال می‌کند.

کیف پول دیجیتال می‌تواند توسـط موجودیت‌های مختلفی ارائه شـود که از این جمله می‌توان به موارد زیر اشاره کرد:

- فروشندگان
- بانک‌های صادرکننده کارت
- ارائه‌دهندگان خدمات پرداخت

نکته دیگر در کاربردهای کیف پول دیجیتال این اسـت که ارائه‌دهنده کیف پول دیجیتال باید مجوز لازم را از بانک‌های صادرکننده کارت‌های تحت پوشش، دریافت نماید.

طبق مطالعات و بررســی‌های انجام شــده عموماً نقش درخواســت‌دهنده نشــانه را ارائه‌دهندگان کیف پول دیجیتال به عهده دارند. بنابراین ارائه‌دهنده کیف پول دیجیتال در صــورتیکه به عنوان درخواســت‌دهنده نشــانه ایفای نقش نماید، باید وظایفی را در مرحله صــدور و اعطای نشــانه انجام دهد. به عبارتی کلیه مســئولیت‌های درخواست‌دهنده نشانه برای ارائه‌دهنده کیف پول دیجیتال در نظر گرفته می‌شود.

ارائه‌دهنده کیف پول دیجیتال در مرحله انجام تراکنش نقشــی ایفا نمی‌کند مگر اینکه، اطلاعات نشــانه در سمت کاربر ذخیره نشده و نیاز به دریافت آن اطلاعات از فضای ابری ارائه‌دهنده کیف پول دیجیتال باشد.

نمونه‌هایی از ارائه‌دهندگان کیف پول دیجیتال شامل موارد زیر هستند:

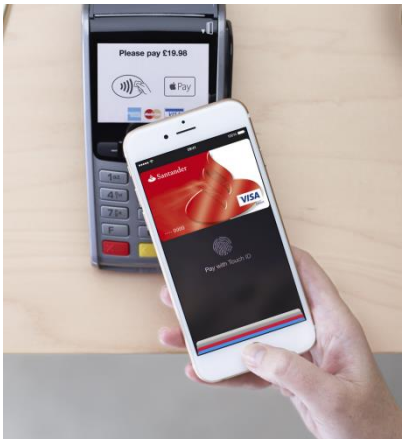
شرکت *Google [7]* نمونه‌ای از ارائه‌دهندگان کیف پول دیجیتال به نام *Google Wallet* است که به عنوان درخواست‌دهنده نشانه در اکوسیستم نشان‌گذاری نقش ایفا می‌نماید. ذخیره‌سازی در *Google Wallet* با استفاده از فناوری *HCE*[1] صورت می‌پذیرد. کاربران می‌توانند با ا ستفاده از این کیف پول اقدام به انتقال وجه و یا ار سال

[1] *Host Card Emulation*

درخواست وجه از افراد دیگر را داشته باشند. بدین منظور تنها کافیست اطلاعات کارت خود را در کیف پول وارد نموده و به یک آدرس ایمیل و یا شماره تلفن همراه وجه مورد نظر را ارسال و یا از آن درخواست وجه نمایند. سپس یک پیغام اطلاع‌رسانی برای گیرنده ارسال خواهد شد. همچنین کاربران *Google Wallet* می‌توانند با استفاده از کیف پول خود در سایت‌های اینترنتی مجهز به نماد *Google Wallet* خرید آسان و امن را تجربه نمایند. در فروشگاه‌هایی که این کیف پول را پشتیبانی می‌نمایند باید نماد *PayPass* بر روی دستگاه کارت خوان آن فروشگاه موجود بوده تا با استفاده از فناوری *NFC* کاربران اقدام به خرید با استفاده از کیف پول خود نمایند. احراز هویت کاربران با استفاده از ورود رمز عبور کیف پول انجام خواهد شد. در شکل ۵ نمونه‌ای از کاربرد *Google Wallet* نشان داده شده است.

شکل ۵- نمونه کاربرد *Google Wallet*

نمونه دیگری از ارائه‌دهندگان کیف پول دیجیتال شرکت *Apple [6]* است. این شرکت با شماری از بانک‌ها قراردادی منعقد نموده و سرویس پرداخت مبتنی بر نشان‌گذاری را با استفاده از بخش *Secure Element* تجهیز همراه به کاربران خود در آن بانک‌ها ارائه می‌دهد. کاربران *Apple* باید کارت‌های بانکی اعم از اعتباری و غیره را در کیف پول همراه گوشی‌های *iPhone* خود اضافه نموده و اطلاعات کارت را در آن وارد نمایند. سپس در برنامه‌های کاربردی و سایت‌های اینترنتی مجهز به نماد *Apple Pay* از خرید آسان و امن بهره ببرند. همچنین در فروشگاه‌ها با استفاده از فناوری *NFC*، کاربران می‌توانند با مجاورت تلفن‌های همراه و دستگاه کارت‌خوان و انجام احراز هویت با *Touch ID* پرداخت‌های خود را انجام دهند.



شکل ۶- نمونه کاربرد *Apple Pay*

۲-۳- سرویس‌دهنده نشانه

سرویس‌دهنده نشانه موجودیت/موجودیت‌هایی درون اکوسیستم نشان‌گذاری است که وظیفه ارائه نشانه‌های پرداخت به درخواست‌دهنده‌گان نشانه را دارد.

سرویس‌دهنده نشانه به عنوان طرف مجاز و صاحب اختیار صدور نشانه‌های پرداخت مسئولیت عملکردهای متفاوت و متعددی را در حوزه توانایی خود دارد. این مسئولیت‌ها شامل و نه محدود به موارد زیر می‌شوند:

- ثبت‌نام *(Registration)* درخواست‌دهنده نشانه: فعالیت‌هایی که برای برقراری ارتباط میان درخواست‌دهنده نشانه و سرویس‌دهنده نشانه مورد نیاز است.
- ثبت‌نام *(Enrollment)* کارت: به موجب این فعالیت شماره کارت کاربر در سامانه پرداخت نشان‌گذاری شده ثبت می‌شود.
- ارتباط با صادرکنندگان به منظور انجام عملیات شناسایی و اعتبارسنجی: به واسطه این فعالیت، صدور نشانه برای شماره کارت مشخص شده توسط بانک تایید یا رد می‌شود.
- صدور *(Issuance)* نشانه: تولید نشانه برای جایگزینی شماره کارت در این فعالیت به انجام می‌رسد.
- اعطای *(Provisioning)* نشانه: براساس فعالیت‌های این قسمت، نشانه تولید شده در مرحله قبل به دارنده کارت تحویل داده می‌شود.

- کنترل و مدیریت شماره شناسایی بانک: به منظور جلوگیری از ایجاد تداخل میان نشانه و شماره کارت باید نحوه صدور نشانه‌ها کنترل شود.
- استقرار و نگهداری مداوم نشانگاه (نگاشت میان شماره کارت و نشانه) به صورت امن: نگهداری از نشانه‌ها در نشانگاه، مستلزم رعایت کردن اصول و الزامات امنیتی است.
- بکاربردن کنترل‌های امنیتی برای محدودسازی کاربرد نشانه: با بکاربردن کنترل‌های امنیتی محدودکننده، اثر وقوع نشت اطلاعات نشانه کاهش خواهد یافت.
- مدیریت کلید: برای رمزنگاری برخی داده‌های تراکنش به منظور کنترل صحت آن‌ها لازم است روال‌هایی برای مدیریت کلید میان سرویس‌دهنده نشانه و درخواست‌دهنده نشانه برقرار شود.
- مدیریت چرخه حیات نشانه: لازم است سازوکاری به منظور ثبت و به‌روزرسانی وضعیت نشانه‌ها در نظر گرفته شود.

- انجام عملیات بازیابی نشانه: در زمان انجام تراکنش مبتنی بر نشانه، لازم است اطلاعات نشانه با اطلاعات کارت جایگزین شده و تراکنش حاوی اطلاعات کارت به بانک صادرکننده ارسال شود.

پیوست یک- واژگان

جدول ۱- واژگان

اصطلاح	معادل انگلیسی	توضیحات
اعطای نشانه	*Token Provisioning*	عمل تحویل نشانه پرداخت و ارزش‌های وابسته آن که به صورت بالقوه شامل یک یا چند کلید رمزی برای تولید رمزنگاشت است- به مکان نشانه می‌باشد.
بازیابی نشانه	*De-Tokenization*	فرآیند بازیابی مقدار شماره کارت مرتبط با یک نشانه پرداخت بر اساس نگاشت آن نشانه پرداخت به شماره کارت که در نشانگاه ذخیره شده است. توانایی بازیابی شماره کارت در ازای نشانه پرداخت مرتبط با آن باید فقط محدود به اختیارات موجودیت‌ها، افراد، برنامه‌های کاربردی و سیستم‌های مجوزدهی شده خاص باشد.
دارنده کارت	*Cardholder*	هر شخصی که برایش یک حساب مالی متصل به کارت توسط بانک صادرکننده ایجاد شده است.
دامنه نشانه	*Token Domain*	انواع تراکنش‌هایی که نشانه پرداخت در آن‌ها قابل استفاده است. دامنه‌های نشانه می‌توانند مختص کانال (برای مثال فقط *NFC*)، مختص صاحب کسب و کار، مختص کیف پول دیجیتال یا ترکیبی از آن‌ها باشند.
درخواست نشانه	*Token Request*	فرآیندی که طی آن درخواست‌دهنده نشانه، یک نشانه پرداخت از سرویس دهنده نشانه درخواست می‌کند.
درخواست‌دهنده نشانه	*Token Requestor*	موجودیتی که به دنبال پیاده‌سازی نشان‌گذاری بوده و با ارائه درخواست خود به سرویس‌دهنده نشانه درخواست تبدیل شماره کارت به نشانه را اعلام می‌کند.
شماره شناسایی بانک	*BIN (Bank Identification Number)*	شماره شناسایی بانک توسط شبکه‌های پرداخت به صادرکنندگان کارت اختصاص داده می‌شود. شماره شناسایی بانک با نیازمندی‌های *ISO 7812* برای شناسایی شبکه پرداخت سازگار هستند.

اصطلاح	معادل انگلیسی	توضیحات
شماره کارت	*PAN*	یک شماره کارت با طول متغیر ۱۳ تا ۱۹ رقم و سازگار با *ISO 7812* است که درون گستره شماره حساب‌های مرتبط با شماره شناسایی بانک صادرکننده کارت تولید می‌شوند.
شناسایی و اعتبارسنجی	*ID&V*	روش معتبری که از طریق آن یک موجودیت بتواند به طور موفقی دارنده کارت و حساب او را راستی‌آزمایی کند تا بتواند به یک سطح اعتماد مناسب برای ایجاد ارتباط بین نشانه پرداخت و شماره کارت/دارنده کارت برسد.
شناسه درخواست‌دهنده نشانه	*Token Requestor ID*	مقداری که به منظور نشان دادن ارتباط پیام احراز هویت/راستی‌آزمایی به یک درخواست دهنده نشانه تعلق می‌گیرد.
صدور نشانه	*Token Issuance*	فرآیندی که در آن نشانه پرداخت ایجاد شده و به درخواست‌کننده نشانه ارائه می‌شود. نشانه‌های پرداخت می‌توانند برای کاربردهای متعدد یا یک کاربرد واحد صادر شوند.
کنترل‌های محدودیت دامنه نشانه	*Token Domain Restriction Controls*	مجموعه‌ای از پارامترها که به عنوان بخشی از صدور نشانه پرداخت توسط سرویس دهنده نشانه وضع شده است و اجازه می‌دهد که کاربرد درست از نشانه پرداخت در تراکنش‌های پرداخت مدیریت شود.
نشانگاه	*Token Vault*	انباره‌ای که توسط سیستم نشان‌گذاری پیاده‌سازی شده و نگاشت بین نشانه پرداخت و شماره کارت را در خود نگهداری می‌کند.

مراجع

[1] EMVCo Payment Tokenisation Specification Technical Framework v1.0, 2014
[2] Information Supplement: PCI DSS Tokenization Guidelines, v2.0, 2011
[3] Let's Talk Tokenization for Mobile Payment Security, Gemalto, 2015
[4] Market Guide for Issuer Tokenization, Gartner, 2015
[5] Market Guide for Merchant/Acquirer Tokenization of Payment Card Data, Gartner, 2015
[6] https://www.apple.com/apple-pay/
[7] https://www.google.com/wallet/