بانک مرکزی جمهوری اسلامی ایران

مدیریت کل فناوری اطلاعات

اداره نظام‌های پرداخت

معماری کلان پرداخت مبتنی بر نشان‌گذاری

نسخه اول

چهارم مرداد ماه هزار و سیصد و نود و شش

شناسنامه سند
نام سند: معماری کلان پرداخت مبتنی بر نشان‌گذاری
نام تهیه‌کننده: بانک مرکزی جمهوری اسلامی ایران
طبقه‌بندی: عادی
تاریخ تهیه: ۱۳۹۶/۰۵/۰۴
نسخه: ۱,۰
تعداد صفحات: ۲۴
پیوست و ضمایم: دارد

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

فهرست مطالب

فهرست اشکال

فهرست جداول

مقدمه

در حال حاضر توسعه و پیشرفت سیستم‌های پرداخت در بکارگیری فناوری‌های نوین با هدف تسهیل انجام عملیات پرداخت، امری انکار ناپذیر است. اگرچه این موضوع موجب بهبود کیفیت و افزایش دسترس‌پذیری خدمات بانکی شده، اما با بوجود آمدن تهدیدات جدید امنیتی حوزه پرداخت، امنیت اطلاعات را با چالش‌های جدی روبرو نموده است. بنابراین همزمان با توسعه خدمات جدید پرداخت، لازم است سازوکارهایی برای تامین امنیت آن‌ها اتخاذ و از وقوع رخدادهای زیان‌بار و جبران‌ناپذیر پیشگیری شود. یکی از راهکارهایی که به منظور تامین امنیت در کانال‌های نوین پرداخت مطرح شده، نشان‌گذاری است.

نشان‌گذاری به عنوان راهکاری در راستای ارتقاء کارایی تراکنش، افزایش سطح امنیت تراکنش یا ارائه روش جدیدی برای گسترش امکان فعالیت شرکت‌های ثالث است که به واسطه آن اکوسیستم جدیدی در سیستم پرداخت معرفی می‌شود. این راهکار به واسطه جایگزینی اطلاعات کارت با نشانه در تراکنش‌های مالی و تعریف نشانه در دامنه بخصوص (مانند کانال پرداخت و فروشنده بخصوص)، ریسک امنیتی افشاء اطلاعات را کاهش می‌دهد. به عبارت دیگر بنابر اعمال محدودیت در استفاده از نشانه، در صورت دسترسی فرد غیرمجاز به اطلاعات نشانه، اثر وقوع رخدادهای امنیتی کاهش خواهد یافت. با توجه به اینکه امنیت اطلاعات از دیدگاه کلیه اعضاء سیستم پرداخت یک چالش مهم است، بکارگیری این راهکار مزایایی را در ایجاد پایداری و سطح امنیت مناسب‌تر برای تمامی آن‌ها در بر خواهد داشت.

پیاده‌سازی راهکار نشان‌گذاری مستلزم ایجاد نقش‌ها و مسئولیت‌های جدیدی است که بواسطه آن‌ها فعالیت‌های جدید حوزه نشان‌گذاری تعریف و اجرا شوند. بنابراین لازم است معماری پرداخت مبتنی بر نشان‌گذاری در کشور با هدف تعریف نقش‌ها، ارتباطات میان نقش‌ها و فرایندهای اجرایی آن‌ها تدوین شود.

مستند پیش رو با عنایت به تصمیمات اتخاذ شده توسط هیئت محترم عامل بانک مرکزی جمهوری اسلامی ایران در خصوص ایجاد زیرساخت امن در پرداخت نشان‌گذاری شده و به منظور ارائه معماری نشان‌گذاری در شبکه بانکی کشور در قالب ۴ بخش، به صورت زیر ارائه گردیده است:

۱. نقش‌های اکوسیستم نشان‌گذاری
۲. ارتباطات اعضاء اکوسیستم نشان‌گذاری
۳. فرایندهای نشان‌گذاری
۴. سناریوی پرداخت مبتنی بر نشان‌گذاری

تعاریف

در این مستند عناوین زیر به جای عبارات مربوطه مورد استفاده قرار خواهند گرفت:

- **بانک مرکزی**: بانک مرکزی جمهوری اسلامی ایران
- **سهند**: سامانه هدایت نشانه‌های دیجیتال
- **بانک**: بانک صادرکننده متقاضی خدمات پرداخت مبتنی بر نشان‌گذاری
- **مانا**: مرکز ارائه نشانه‌های الکترونیکی
- **دنا**: درخواست‌دهنده نشانه‌های الکترونیکی

معماری کلان پرداخت مبتنی بر نشان‌گذاری

در این مستند براساس دستورالعمل بانک مرکزی در خصوص ایجاد زیرساخت امن پرداخت‌های نشان‌گذاری شده با شماره نامه ۹۶/۲۷۰۶۵م مورخ ۲/۴/ ۱۳۹۶، معماری کلان راهکار نشان‌گذاری مورد بررسی قرار گرفته است. بکارگیری راهکار نشان‌گذاری در هر سیستم پرداخت مستلزم ایجاد نقش‌هایی است که فعالیت‌های چارچوب نشان‌گذاری را به انجام رسانند. لذا در این مستند پس از بررسی نقش‌های اکوسیستم پرداخت مبتنی بر نشان‌گذاری در کشور، ارتباطات میان اعضاء اکوسیستم نشان‌گذاری و فرایندهای اجرایی آن‌ها مورد توجه قرار خواهد گرفت.

۱- نقش‌های اکوسیستم نشان‌گذاری

نقش‌های اکوسیستم پرداخت مبتنی بر نشان‌گذاری در کشور شامل ۴ نقش بانک، دنا، سهند و مانا است که در ادامه به شرح وظایف هر یک از نقش‌ها پرداخته شده است.

۱-۱- بانک

لازم است بانک‌ها در صورت تمایل به ایفای نقش در اکوسیستم نشان‌گذاری فعالیت‌های زیر را انجام دهند:

- انجام ثبت‌نام در سامانه سهند به منظور استفاده از خدمات سهند و فعالیت در پرداخت مبتنی بر نشان‌گذاری
- انجام ممیزی‌های عملکردی و امنیتی دنا و مانا به منظور حصول اطمینان از صحت عملکرد و برقراری امنیت در سیستم‌های آن‌ها
- معرفی دنا و مانا به سامانه سهند برای انجام فرایندهای نشان‌گذاری میان سهند، دنا و مانا
- ارائه واسط نرم‌افزاری به سهند برای انجام عملیاتی مانند فرایند شناسایی و اعتبارسنجی درخواست صدور نشانه
- انجام بخشی از عملیات شناسایی و اعتبارسنجی در ارتباط با سهند به منظور تایید یا رد اعتبار درخواست نشانه
- ارائه خدمات پشتیبانی به مشتریان متقاضی استفاده از پرداخت مبتنی بر نشان‌گذاری
- تعیین سیاست‌های بانکی صدور نشانه برای مانا مانند مدت اعتبار نشانه

۱-۲- دنا

دنا با هدف اجرای فعالیت‌های درخواست‌دهنده نشانه وظایف زیر را عهده‌دار خواهد بود:

- اخذ مجوز فعالیت در حوزه نشان‌گذاری از حداقل یک بانک فعال در حوزه نشان‌گذاری به منظور برقراری اتصال با سهند
- تعیین دامنه فعالیت در حوزه نشان‌گذاری (مانند پرداخت از طریق NFC و پرداخت درون‌برنامه‌ای[1])
- ارائه درخواست تبدیل اطلاعات کارت به نشانه از طرف دارنده کارت به سامانه سهند
- ذخیره سازی نشانه به صورت امن و رعایت الزامات و کنترل‌های امنیتی
- عدم ذخیره‌سازی اطلاعات کارت و همچنین نگاشت میان نشانه و شماره کارت
- پیاده‌سازی عملیات مربوط به مدیریت کلید طبق دستورالعمل سهند
- ارائه درخواست دارنده کارت به سامانه سهند به منظور ثبت و به‌روزرسانی وضعیت کارت
- ارسال درخواست به‌روزرسانی وضعیت نشانه به سامانه سهند

۱-۳- سهند

سامانه سهند به عنوان سامانه حاکمیتی به منظور انجام بخش عمده‌ای از فعالیت‌های سرویس‌دهنده نشانه، وظایف زیر را انجام خواهد داد:

- ارائه الزامات حوزه نشان‌گذاری با هدف برقراری امنیت، پایداری و یکپارچگی سرویس
- ارائه سرویس اتصال برخط بانک، دنا و مانا به سیستم پرداخت مبتنی بر نشان‌گذاری به صورت متمرکز
- اتصال برخط با شتاب برای انجام تراکنش‌های مبتنی بر نشانه
- مسیردهی پیام‌ها در شبکه نشان‌گذاری میان بانک، دنا و مانا
- انجام عملیات ثبت‌نام دنا و مانا براساس مجوز صادرشده توسط بانک

[1] In-App

- ایجاد و تخصیص شناسه دنا به صورت منحصربفرد برای هر دامنه فعالیت (به عبارت دیگر دنا در صورت تمایل به فعالیت در دو حوزه NFC و پرداخت درون‌برنامه‌ای دو شناسه منحصربفرد از سامانه سهند دریافت می‌کند.)
- انجام عملیات ثبت‌نام کارت در سیستم نشان‌گذاری به منظور صدور نشانه برای آن
- تهیه دستورالعمل فنی واسط‌های نرم افزاری برای برقراری ارتباط با دنا، مانا و بانک در پرداخت مبتنی بر نشان‌گذاری
- اعطای نشانه صادرشده توسط مانا به دنا
- انجام عملیات شناسایی و اعتبارسنجی در ارتباط با بانک صادرکننده کارت به منظور تایید اعتبار درخواست صدور نشانه براساس یک یا چند مورد زیر:
  - سطح ۱. عدم انجام فرایند شناسایی و اعتبارسنجی: صدور نشانه بدون انجام عملیات شناسایی و اعتبارسنجی
  - سطح ۲. تایید اعتبار اطلاعات کارت توسط بانک: تایید شماره کارت، تاریخ انقضای کارت و CVV/CVV2
  - سطح ۳. تایید اعتبار درخواست صدور نشانه براساس ریسک: ارزیابی ریسک براساس اطلاعاتی چون سابقه فعالیت کارت، موقعیت جغرافیایی دارنده کارت و سابقه دنای ارسال‌کننده درخواست
  - سطح ۴. احراز هویت دارنده کارت به صورت خارج از کانال: ارسال رمز یکبار مصرف[1]، ایمیل و استفاده از سامانه 3D-Secure ACS
- مدیریت BIN نشانه‌ها به منظور جلوگیری از تداخل نشانه و اطلاعات کارت موجود در شبکه بانکی و همچنین جلوگیری از تداخل نشانه‌ها با یکدیگر
- مدیریت کلیدهای رمزنگاری به منظور برقراری امنیت در نشان‌گذاری
- اعمال کنترل‌های محدودیت دامنه نشانه براساس موارد زیر با هدف تایید کاربرد نشانه در دامنه مجاز (لازم بذکر است، انجام تراکنش منوط به برقراری این کنترل‌ها است):
  - شناسه دنا: هر نشانه تنها برای دنای درخواست‌دهنده آن قابل استفاده است.

[1] One Time Password (OTP)

- روش ورود اطلاعات در پایانه انجام‌دهنده تراکنش: کاربرد هر نشانه محدود به روش مورد توافق در زمان ثبت نام دنا مانند NFC و پرداخت درون‌برنامه‌ای است که این شاخص براساس فیلد "کد روش ورود اطلاعات در پایانه" در تراکنش کنترل می‌شود.
- اطلاعات فروشنده: در شرایطی که فروشنده عهده‌دار نقش دنا است، باید هر فروشنده براساس شناسه از سایر فروشندگان متمایز شود.

- تعیین سطح ضمانت نشانه براساس نحوه انجام عملیات شناسایی و اعتبارسنجی و سایر کنترل‌های امنیتی اعمال شده هنگام صدور نشانه
- عدم ذخیره‌سازی اطلاعات کارت و همچنین نگاشت میان نشانه و شماره کارت

جدول ۱- روش‌های شناسایی و اعتبارسنجی

روش‌های شناسایی و اعتبارسنجی	توضیحات
بدون شناسایی و اعتبارسنجی	-
تایید اطلاعات کارت	بررسی اعتبار اطلاعات کارت اعم از شماره کارت، تاریخ انقضای کارت و CVV/CVV2
شناسایی و اعتبارسنجی مبتنی بر ریسک	ارزیابی ریسک براساس اطلاعاتی چون سابقه فعالیت کارت، موقعیت جغرافیایی دارنده کارت و سابقه دنای ارسال‌کننده درخواست
احراز هویت دارنده کارت	احراز هویت دارنده کارت براساس روش خارج از کانال ارائه درخواست، مانند ارسال رمز یکبار مصرف و ایمیل

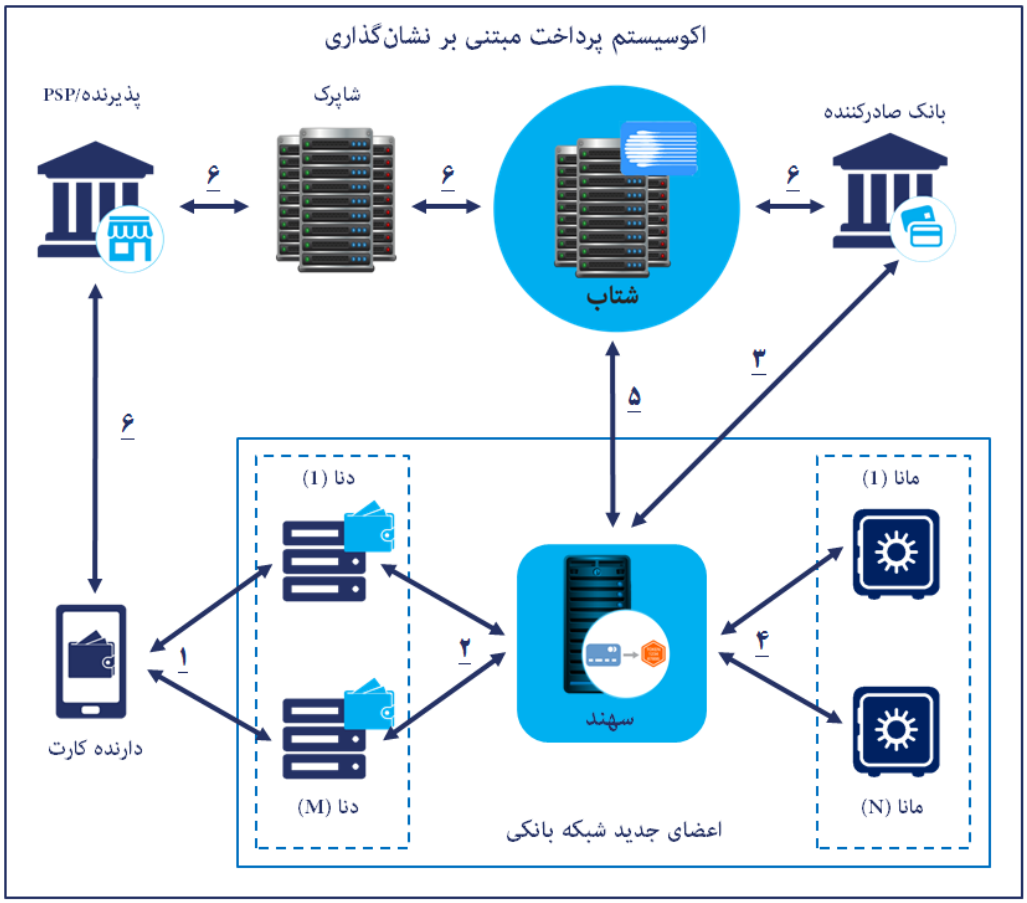
۱-۴- مانا

مانا به عنوان مخزن ذخیره شماره‌های کارت، نشانه‌ها و تناظر میان آن‌ها وظایف زیر را به عهده دارد:

- اخذ مجوز فعالیت از حداقل یک بانک فعال در حوزه نشان‌گذاری به منظور برقراری اتصال با سهند
- صدور نشانه پرداخت
- نگهداری امن از اطلاعات کارت و نشانه و رعایت الزامات و کنترل‌های امنیتی
- بازیابی شماره کارت از نشانه در زمان پرداخت
- اعمال پارامترهای اعتبار نشانه براساس سیاست‌های بانک و سهند
- به‌روزرسانی وضعیت نشانه براساس حالت‌های فعال، موقتا غیرفعال و غیرفعال

۲- ارتباطات اعضاء اکوسیستم نشان‌گذاری

پس از مشخص شدن نقش‌های اکوسیستم نشان‌گذاری، در این بخش از مستند نحوه ارتباط اعضاء این اکوسیستم در معماری نشان‌گذاری مورد توجه قرار خواهد گرفت. طبق طرح معماری موجود در شکل ۱، کلیه ارتباطات دنا و مانا با سیستم پرداخت و بالعکس تنها از طریق سهند برقرار شده است. در واقع سهند از یک سو با جلوگیری از پراکندگی و نابسامانی در اتصالات میان بخش درخواست‌دهنده سرویس و ارائه‌دهنده سرویس، نقش یک موجودیت متمرکز نظم‌دهنده در معماری نشان‌گذاری را ایفا می‌کند و از سوی دیگر با انجام بخش قابل توجهی از فعالیت‌های ارائه‌دهنده سرویس، پیاده‌سازی این راهکار را به شیوه‌ای کنترل‌شده، استاندارد و امن میسر می‌سازد. همچنین سهند به عنوان تعیین‌کننده الزامات حوزه نشان‌گذاری موجب یکپارچگی فرایندها در مانا و دنا خواهد بود. در شکل ۱ لینک‌های ارتباطی و کاربرد آن‌ها به صورت کلی مورد بررسی قرار گرفته است.



شکل ۱- معماری کلان پرداخت مبتنی بر نشان‌گذاری

ارتباطات میان اعضاء سیستم پرداخت مبتنی بر نشان‌گذاری طبق شکل ۱ به شرح زیر می‌باشد:

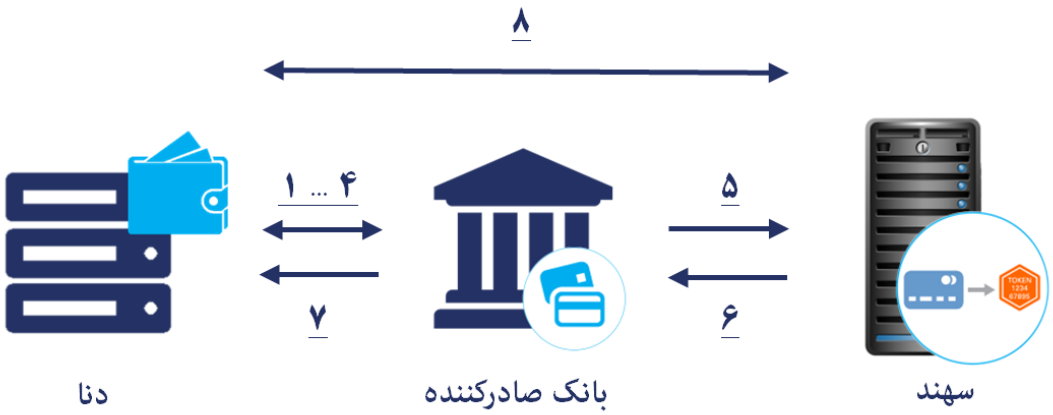
۱. ارتباط دارنده کارت با دنا:
   - درخواست ثبت شماره کارت در پرداخت مبتنی بر نشان‌گذاری از سوی دارنده کارت
   - اعطای نشانه از دنا به دارنده کارت
   - درخواست تغییر وضعیت نشانه
۲. ارتباط دنا با سهند:
   - ارسال درخواست ثبت شماره کارت و صدور نشانه از دنا به سهند
   - ارسال نشانه از سهند به دنا
   - ارسال درخواست تغییر وضعیت نشانه
۳. ارتباط میان سهند و بانک به منظور کسب مجوز صدور نشانه برای شماره کارت
۴. ارتباط میان سهند و مانا:
   - درخواست صدور نشانه از سهند به مانا
   - ارسال نشانه از مانا به سهند برای اعطا به دارنده کارت
   - ارسال درخواست بازیابی شماره کارت متناظر با نشانه از سهند به مانا
   - ارسال درخواست تغییر وضعیت نشانه از سهند به مانا
۵. ارتباط شتاب با سهند به منظور جایگزینی اطلاعات نشانه با اطلاعات کارت در انجام تراکنش
۶. ارتباطات موجود در شبکه بانکی به منظور انجام تراکنش

۳- فرایندهای نشان‌گذاری

در این بخش از مستند فرایندهای نشان‌گذاری به طور کلی مورد بررسی قرار گرفته است.

۳-۱- ثبت‌نام دنا در سهند

یکی از مراحل اولیه برای آغاز فعالیت‌های نشان‌گذاری، ثبت‌نام شرکت‌های مجاز برای ایفای نقش دنا است. کسب‌وکارهای مجازی که چنین درخواستی دارند باید مطابق شکل ۲ از طریق بانک طرف قرارداد خود طی گام‌های زیر اقدام به ثبت‌نام نمایند:



شکل ۲- فرایند ثبت‌نام دنا

۱- دنا درخواست ثبت‌نام را به بانک طرف قرارداد خود ارائه می‌دهد.

۲- بانک با ارائه فرم‌هایی به دنا، اطلاعات زیر را کسب می‌کند:

- اطلاعات مرتبط با کسب‌وکار دنا و زمینه فعالیت آن
- دامنه فعالیت کسب‌وکار دنا در حوزه نشان‌گذاری، اعم از فعالیت در حوزه پرداخت از طریق NFC یا پرداخت درون‌برنامه‌ای
- نحوه ذخیره‌سازی اطلاعات نشانه (ذخیره‌سازی در برنامه کاربردی، فضای ابری و ...)
- اسناد بالادستی مرتبط با کسب و کار دنا

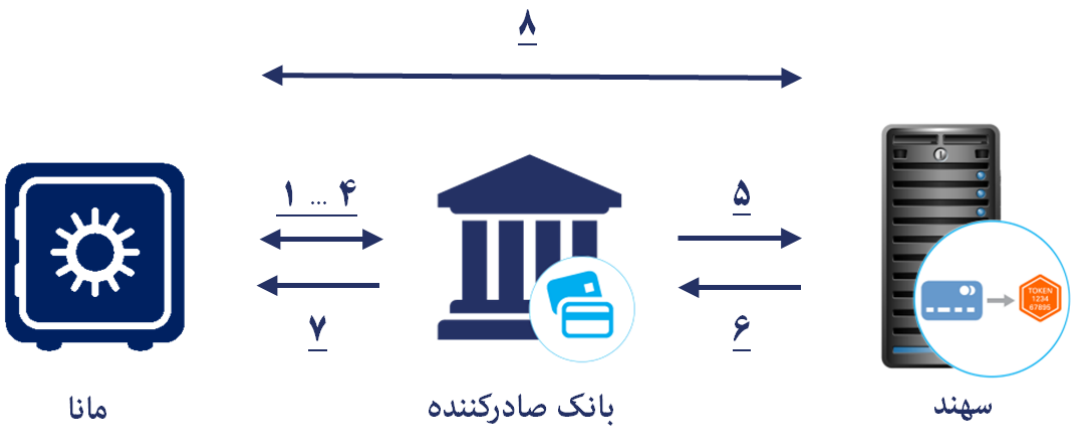
۳- بانک الزامات تعیین‌شده توسط بانک مرکزی را به دنا ابلاغ می‌نماید.

۴- بانک پس از بررسی اطلاعات دریافتی و با توجه به چک لیست‌ها و الزاماتی که برای ممیزی امنیتی دنا در نظر گرفته شده است، صلاحیت کسب‌وکار آن را مورد بررسی قرار می‌دهد.

۵- در صورت تایید، بانک نام شرکت/موسسه درخواست‌دهنده را به اطلاع سهند رسانده و سهند شناسه منحصر بفردی را برای دنا صادر می‌نماید.
۶- سهند شناسه صادرشده را به همراه سایر اطلاعات مورد نیاز برای برقراری ارتباط میان سهند و دنا به بانک ارائه می‌دهد.
۷- بانک تائیدیه ثبت‌نام را به دنا اطلاع می‌دهد.
۸- ارتباط میان سهند و دنا از طریق واسط نرم‌افزاری ارائه‌شده برقرار می‌شود.

۳-۲- ثبت‌نام مانا در سهند

مانا پس از انجام موفقیت‌آمیز گام‌های زیر مطابق با شکل ۳، قادر است فعالیت خود را در حوزه نشان‌گذاری آغاز کند:



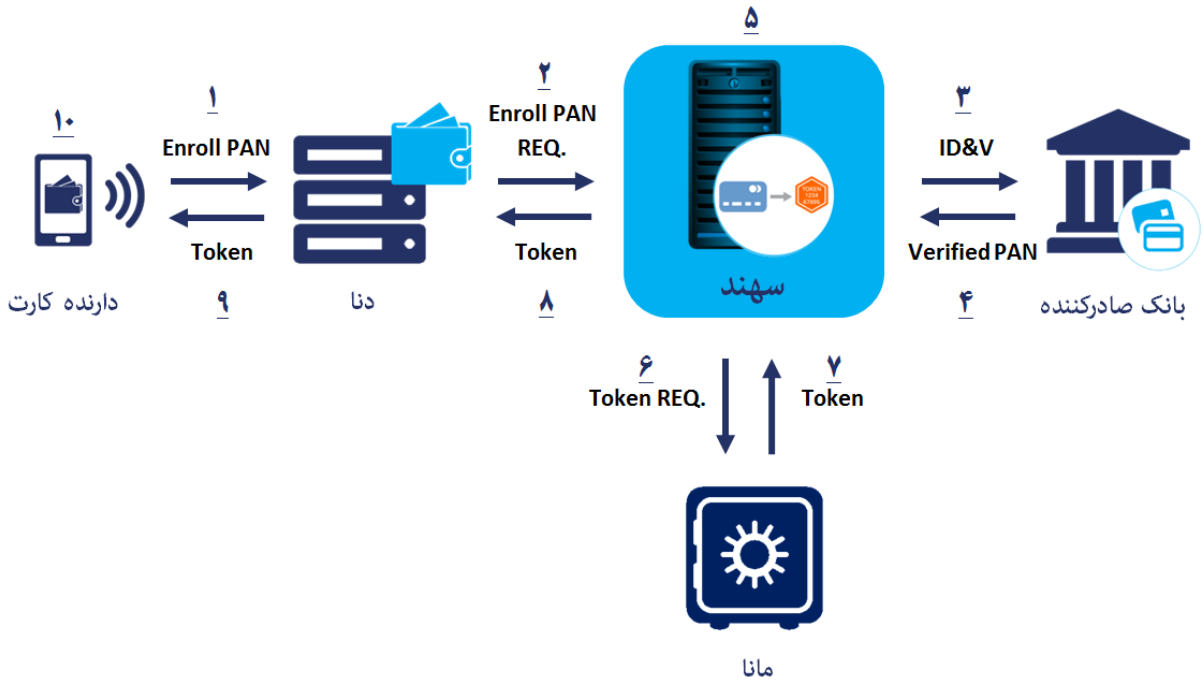
شکل ۳- فرایند ثبت‌نام مانا

۱- مانا درخواست آغاز فعالیت را به بانک طرف قرارداد خود ارائه می‌دهد.
۲- بانک الزامات تعیین شده توسط بانک مرکزی (مانند الزامات فرایندی و امنیتی نگهداری از اطلاعات کارت و نشانه) را به مانا ارائه می‌دهد.
۳- بانک با توجه به چک لیست‌ها و الزاماتی که برای ممیزی مانا در نظر گرفته شده، به نحوی صلاحیت مانا را مورد بررسی قرار می دهد.
۴- در صورت تایید، بانک دستورالعمل فنی سهند را به منظور تهیه واسط نرم‌افزاری در اختیار مانا قرار می‌دهد.
۵- بانک اطلاعات مورد نیاز برای برقراری ارتباط با مانا را در اختیار سهند قرار می‌دهد.

۶- سهند پس از انجام آزمون صحت کارکرد مانا نتیجه را در اختیار بانک قرار می‌دهد.
۷- بانک تائیدیه ثبت‌نام را به مانا اطلاع می‌دهد و محدوده مجاز شماره شناسایی بانک را که سهند برای آن بانک تعیین می‌نماید، به مانا اعلام می‌کند.
۸- ارتباط میان سهند و مانا از طریق واسط نرم‌افزاری ارائه‌شده برقرار می‌شود.

۳-۳- صدور و اعطای نشانه

در این مرحله دارنده کارت، درخواست خود برای استفاده از خدمات پرداخت مبتنی بر نشان‌گذاری را ارائه می‌دهد. عملیات صدور و اعطای نشانه به دارنده کارت طبق شکل ۴ در مراحل زیر انجام می‌پذیرد:



شکل ۴- فرایند صدور و اعطای نشانه

۱- دارنده کارت درخواست ثبت‌نام کارت را صادر می‌کند.
۲- دنا پس از دریافت اطلاعات از دارنده کارت، یک درخواست ثبت‌نام کارت به سهند ارسال می‌کند.
۳- سهند برای دریافت مجوز صدور نشانه درخواست شناسایی و اعتبارسنجی را به بانک ارسال می‌کند.
۴- بانک براساس یک یا مجموعه‌ای از سطوح شناسایی و اعتبارسنجی، مجوز صدور نشانه را بررسی نموده و نتیجه را به سهند ارائه می‌دهد.

۵- سهند بر اساس متد شناسایی و اعتبارسنجی، سطح ضمانت نشانه را تعیین می‌کند و برای عدم ذخیره‌سازی اطلاعات کارت، یک شناسه با عنوان PANUniqueReference را که برای هر کارت منحصر بفرد است تولید می‌کند.
۶- سهند براساس شماره شناسایی بانک، درخواست صدور نشانه را به مانای بانک صادرکننده کارت ارسال می‌کند.
۷- مانا برای کارت درخواست شده یک نشانه تولید می‌کند و تناظر میان اطلاعات کارت، PANUniqueReference، نشانه و شناسه دنا را نگهداری نموده و نشانه صادر شده را به سهند تحویل می‌دهد.
۸- سهند نشانه صادر شده را به همراه PANUniqueReference به دنا تحویل می‌دهد.
۹- دنا براساس سیاست تعیین شده در ذخیره‌سازی نشانه، اطلاعات زیر را ذخیره می‌کند:
- نشانه
- تاریخ انقضای نشانه
- کلید
- شناسه دنا

۱۰- دارنده کارت از پایان یافتن عملیات ثبت کارت در سامانه پرداخت مبتنی بر نشان‌گذاری توسط دنا مطلع می‌شود.

۳-۴- مدیریت چرخه حیات نشانه

در صورت وقوع هر یک از موارد زیر وضعیت نشانه نیازمند به‌روزرسانی است:

- غیرفعال کردن ثبت‌نام در سامانه پرداخت مبتنی بر نشان‌گذاری
- گم/دزدیده شدن تلفن همراه
- نشت اطلاعات کارت یا نشانه
- آلوده‌شدن تلفن همراه به بدافزار

در هر یک از شرایط مذکور لازم است دارنده کارت براساس یکی از روش‌های زیر وضعیت نشانه را به‌روزرسانی کند:

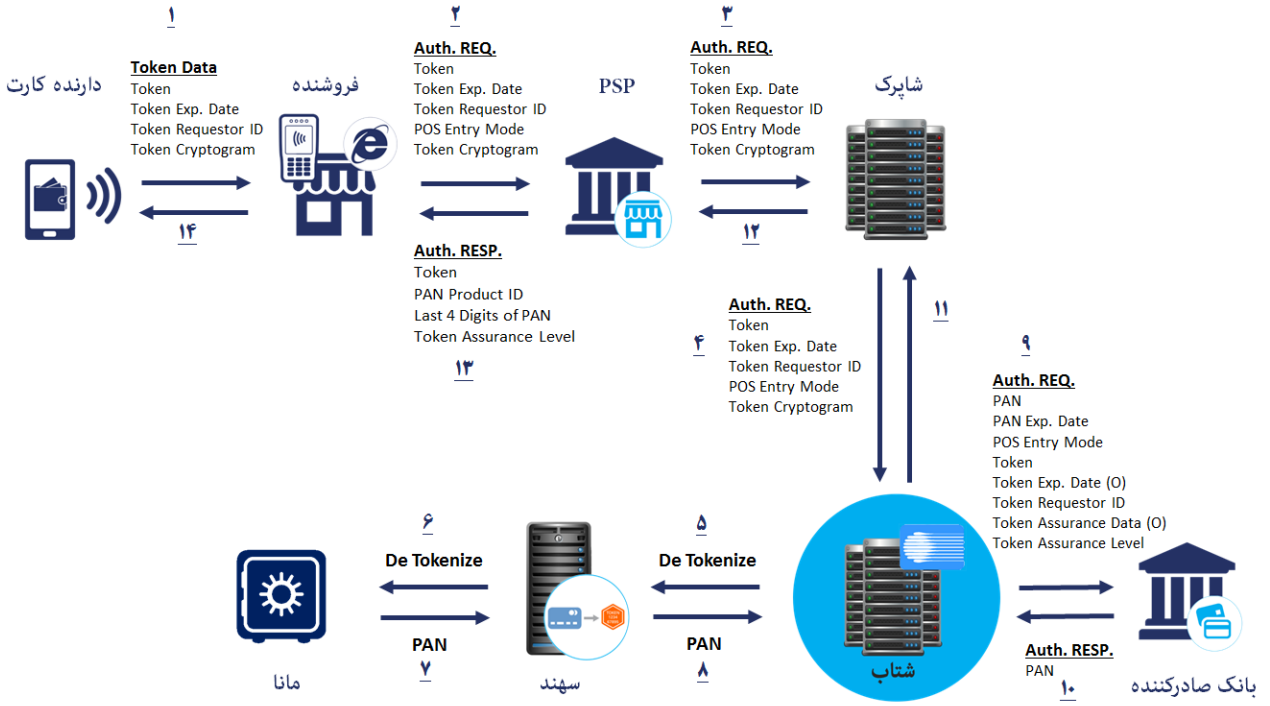
- مراجعه به بانک صادرکننده: در این حالت درخواست دارنده کارت، بر روی پذیرش یا رد کلیه تراکنش‌های آتی مربوط به آن نشانه توسط بانک اثرگذار است.

- استفاده از امکاناتی که دنا برای این منظور در نظر گرفته (به عنوان نمونه غیرفعال کردن کارت توسط کیف پول دیجیتال): دنا پیام به‌روزرسانی وضعیت نشانه را به سهند ارسال کرده و سهند براساسBIN نشانه، آن را به مانای مربوطه تحویل می‌دهد. در نهایت مانا وضعیت نشانه را به‌روزرسانی می‌نماید.

همچنین در شرایطی که دنا تقاضای به‌روزرسانی وضعیت نشانه‌های خود را داشته باشد این درخواست را به سهند ارسال کرده و سهند آن را به مانای مربوطه تحویل داده و وضعیت نشانه‌ها به‌روزرسانی می‌شود.

۴- سناریوی پرداخت مبتنی بر نشان‌گذاری

در این بخش از مستند، انجام عملیات پرداخت مبتنی بر نشان‌گذاری در قالب سناریو شرح داده شده است. این سناریو دو نوع پرداخت از طریق NFC و پرداخت درون‌برنامه‌ای را پوشش می‌دهد. شکل ۵ نشان‌دهنده داده‌های ارسالی در تراکنش‌های مبتنی بر نشانه است. لازم بذکر است استفاده از داده‌های نشان‌داده شده با (O) در تراکنش، اختیاری محسوب می‌شود.



(O): Optional داده‌هایی که استفاده از آن‌ها در تراکنش اختیاری است

شکل ۵- سناریوی پرداخت مبتنی بر نشان‌گذاری

مراحل انجام عملیات پرداخت مبتنی بر نشانه به شرح زیر می‌باشد:

۱- دارنده کارت برای نمونه با استفاده از کیف پول دیجیتال به صورت پرداخت درون‌برنامه‌ای یا پرداخت از طریق NFC اقدام به خرید می‌کند. کیف پول دیجیتال، اطلاعات نشانه، تاریخ انقضای نشانه، رمزنگاشت و شناسه دنا را به منظور آغاز یک تراکنش خرید به ترمینال فروشنده ارسال می‌کند. در این مرحله رمزنگاشت براساس اطلاعات منحصر بفرد هر تراکنش، به منظور کنترل صحت داده‌های تراکنش و جلوگیری از انجام مجدد تراکنش، ایجاد و در تراکنش درج می‌شود.

۲- فروشنده با درج روش ورود اطلاعات در پایانه انجام دهنده تراکنش[1] و سایر داده‌های مورد نیاز، تراکنش حاوی نشانه را صادر کرده و آن را به PSP تحویل می‌دهد.

۳- PSP تراکنش مبتنی بر نشانه را به سوئیچ شاپرک ارسال می‌کند.

۴- سوئیچ شاپرک تراکنش مبتنی بر نشانه را به سوئیچ شتاب ارسال می‌کند.

۵- سوئیچ شتاب با مشاهده BIN نشانه، تراکنش حاوی نشانه را در قالب درخواست بازیابی نشانه به سهند ارسال می‌کند. در این مرحله اطلاعات مربوط به کنترل دامنه نشانه مانند شناسه دنا، روش ورود اطلاعات در پایانه انجام دهنده تراکنش و رمزنگاشت توسط سهند بررسی می‌شود. در صورت تایید موارد امنیتی تراکنش توسط سهند، مراحل آتی ادامه می‌یابد.

۶- سهند براساس BIN نشانه، درخواست بازیابی نشانه را به مانای مناسب ارسال می‌کند.

۷- مانا شماره کارت و سایر اطلاعات کارت متناظر با نشانه را بازیابی کرده و آن را به سهند تحویل می‌دهد.

۸- سهند شماره کارت، سایر اطلاعات کارت، سطح ضمانت نشانه و نشانه (در شرایطی که بانک بخواهد از نشانه صادرشده برای شماره کارت و سطح ضمانت آن اطلاع داشته باشد) را به شتاب تحویل می‌دهد.

۹- شتاب نشانه را با اطلاعات کارت جایگزین کرده و تراکنش حاوی شماره کارت و سایر اطلاعات کارت را در قالب درخواست تایید و بررسی به بانک صادرکننده ارسال می‌کند.

۱۰- بانک صادرکننده تراکنش را تایید یا رد می‌کند و پاسخ را به شتاب تحویل می‌دهد.

۱۱- شتاب به نحوی اطلاعات کارت را با اطلاعات نشانه جایگزین و در صورت لزوم ۴ رقم آخر شماره کارت را نیز در تراکنش درج می‌کند و تراکنش پاسخ را به سوئیچ شاپرک تحویل می‌دهد.

۱۲- سوئیچ شاپرک پاسخ را به سوئیچ PSP تحویل می‌دهد.

۱۳- سوئیچ PSP پاسخ را به ترمینال فروشنده تحویل می‌دهد.

۱۴- دارنده کارت از پاسخ تراکنش مطلع می‌شود.

[1] POS Entry Mode

پیوست یک- واژگان

جدول ۲- واژگان

اصطلاح	معادل انگلیسی	توضیحات
BIN نشانه	Token BIN	یک شماره شناسایی بانک مشخص که تنها با هدف صدور نشانه‌های پرداخت طراحی شده و متناظر با آن در جداول شماره شناسایی بانک علامت‌گذاری شده است.
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 اطلاعات کارت مرتبط با یک نشانه پرداخت بر اساس نگاشت آن نشانه پرداخت به اطلاعات کارت که در نشانگاه ذخیره شده است. توانایی بازیابی اطلاعات کارت در ازای نشانه پرداخت مرتبط با آن باید فقط محدود به اختیارات موجودیت‌ها، افراد، برنامه‌های کاربردی و سیستم‌های مجوزدهی شده خاص باشد.
تاریخ انقضاء نشانه	Token Expiry Date	تاریخ انقضاء نشانه پرداخت توسط نشانگاه تولید شده و در آن نگهداری می‌شود و در زمان پردازش تراکنش برای اطمینان از قابلیت تعامل متقابل و به‌حداقل‌رسانی تأثیر پیاده‌سازی نشان‌گذاری به فیلد تاریخ انقضاء کارت منتقل می‌شود. تاریخ انقضاء نشانه یک ارزش عددی چهار رقمی است که با فرمت ISO 8583 سازگار است.
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.

اصطلاح	معادل انگلیسی	توضیحات
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 را به نشانه اعلام می‌کند.
رمزنگاشت	Cryptogram	یک رمزنگاشت با استفاده از نشانه پرداخت و داده‌های دیگر تراکنش تولید می‌شود تا یک مقدار منحصربفرد برای هر تراکنش ایجاد شود. محاسبات و فرمت رمزنگاشت در هر مورد استفاده متفاوت است.
روش ورود اطلاعات در پایانه انجام‌دهنده تراکنش	POS Entry Modes	روشی که به موجب آن نشانه و اطلاعات مربوط به آن به پای‌انه انجام‌دهنده تراکنش ارسال می‌شود.
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.
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 اطلاعات کارت/دارنده کارت برسد.
شناسه دنا	Token Requestor ID	مقداری که به منظور نشان دادن ارتباط پیام احراز هویت/راستی‌آزمایی به دنا تعلق می‌گیرد.

اصطلاح	معادل انگلیسی	توضیحات
صدور نشانه	Token Issuance	فرآیندی که در آن نشانه پرداخت ایجاد شده و به درخواست-کننده 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.
نشانه پرداخت	Payment Token	نشانه‌های پرداخت می‌توانند در سطح صنعت پرداخت، شکل-های مختلفی به خود بگیرند. در این مشخصات، اصطلاح نشانه پرداخت به ارزش جایگزین شماره کارت گفته می‌شود که یک ارزش عددی ۱۳ تا ۱۹ رقمی است و باید از قوانین راستی-آزمایی پایه نظیر چک ارقام Luhn برای یک شماره حساب بگذرد. نشانه‌های پرداخت در گستره شماره شناسایی بانک تولید می‌شوند که به عنوان BIN نشانه طراحی شده و به تناظر در تمامی جداول شماره شناسایی بانک علامت‌گذاری می‌شوند. نشانه‌های پرداخت نباید ارزششان شبیه یا در تداخل با شماره کارت واقعی باشد.

مراجع

[1] EMVCo Payment Tokenisation Specification Technical Framework v1.0, 2014
[2] https://www.apple.com/apple-pay/
[3] https://www.google.com/wallet/
[4] دستورالعمل بانک مرکزی جمهوری اسلامی در خصوص ایجاد زیرساخت امن پرداخت‌های نشان‌گذاری شده با شماره نامه ۹۶/۲۷۰۶۵م مورخ ۱۳۹۶/۲/۴