



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 نشان گذاری
نام تهیه کننده: بانک مرکزی جمهوری اسلامی ایران
طبقه بندی: حساس
تاریخ تهیه: ۱۳۹۶/۰۵/۰۴
نسخه: ۱,۰
تعداد صفحات: ۲۴
پیوست و ضمایم: دارد

کنترل نسخ مستندات			
نسخه	موضوع بازنگری	تاریخ بازنگری	تهیه کننده
-	-	-	-

حقوق معنوی

این مستند توسط بانک مرکزی جمهوری اسلامی ایران تهیه و تنظیم شده است. لذا هر نوع دسترسی یا استفاده از این مستند توسط اشخاص ثالث، بدون مجوز کتبی "بانک مرکزی جمهوری اسلامی ایران" ممنوع است.

فهرست مطالب

۶	مقدمه
۷	تعاریف
۸	معماری کلان پرداخت مبتنی بر نشان گذاری
۸	۱- نقش های اکوسیستم نشان گذاری
۸	۱-۱- بانک
۹	۲-۱- دنا
۹	۳-۱- سهند
۱۱	۴-۱- مانا
۱۲	۲- ارتباطات اعضاء اکوسیستم نشان گذاری
۱۴	۳- فرایندهای نشان گذاری
۱۴	۳-۱- ثبت نام دنا در سهند
۱۵	۳-۲- ثبت نام مانا در سهند
۱۶	۳-۳- صدور و اعطای نشانه
۱۷	۴-۳- مدیریت چرخه حیات نشانه
۱۹	۴- سناریوی پرداخت مبتنی بر نشان گذاری
۲۱	پیوست یک- واژگان
۲۴	مراجع

فهرست اشکال

- شکل ۱- معماری کلان پرداخت مبتنی بر نشان گذاری ۱۲
- شکل ۲- فرایند ثبت نام دنا ۱۴
- شکل ۳- فرایند ثبت نام مانا ۱۵
- شکل ۴- فرایند صدور و اعطای نشانه ۱۶
- شکل ۵- سناریوی پرداخت مبتنی بر نشان گذاری ۱۹

پایس

پایس

فهرست جداول

- جدول ۱- روش های شناسایی و اعتبارسنجی ۱۱
- جدول ۲- واژگان ۲۱

پیش نویس

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، نشان گذاری است.

نشان گذاری 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 نشان گذاری مستلزم ایجاد نقش‌ها و مسئولیت‌های جدیدی است که بواسطه آن‌ها فعالیت‌های جدید حوزه نشان گذاری تعریف و اجرا شوند. بنابراین لازم است معماری پرداخت مبتنی بر نشان گذاری 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 نشان گذاری شده و به منظور ارائه معماری نشان گذاری در شبکه بانکی کشور در قالب ۴ بخش، به صورت زیر ارائه گردیده است:

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

تعاریف

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

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

معماری کلان پرداخت مبتنی بر نشان گذاری

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

۱- نقش های اکوسیستم نشان گذاری

نقش های اکوسیستم پرداخت مبتنی بر نشان گذاری در کشور شامل ۴ نقش بانک، دنا، سهند و مانا است که در ادامه به شرح وظایف هر یک از نقش ها پرداخته شده است.

۱-۱- بانک

لازم است بانک ها در صورت تمایل به ایفای نقش در اکوسیستم نشان گذاری فعالیت های زیر را انجام دهند:

- انجام ثبت نام در سامانه سهند به منظور استفاده از خدمات سهند و فعالیت در پرداخت مبتنی بر نشان گذاری
- انجام ممیزی های عملکردی و امنیتی دنا و مانا به منظور حصول اطمینان از صحت عملکرد و برقراری امنیت در سیستم های آنها
- معرفی دنا و مانا به سامانه سهند برای انجام فرایندهای نشان گذاری میان سهند، دنا و مانا
- ارائه واسط نرم افزاری به سهند برای انجام عملیاتی مانند 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 نشان گذاری
- تعیین سیاست های 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 نشان گذاری از حداقل یک بانک فعال در حوزه نشان گذاری به منظور برقراری اتصال با سهند
- تعیین دامنه فعالیت در حوزه نشان گذاری (مانند پرداخت از طریق NFC و پرداخت درون برنامه‌ای^۱)
- 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 ذخیره سازی اطلاعات کارت و همچنین نگاشت میان نشانه و شماره کارت
- پیاده سازی عملیات مربوط به مدیریت کلید طبق دستورالعمل سهند
- ارائه درخواست دارنده کارت به سامانه سهند به منظور ثبت و به روز رسانی وضعیت کارت
- ارسال درخواست به روز رسانی وضعیت نشانه به سامانه سهند

۱-۳- سهند

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

- ارائه الزامات حوزه نشان گذاری با هدف برقراری امنیت، پایداری و یکپارچگی سرویس
- ارائه سرویس اتصال برخط بانک، دنا و مانا به سیستم پرداخت مبتنی بر نشان گذاری به صورت متمرکز
- اتصال برخط با شتاب برای انجام تراکنش‌های مبتنی بر نشانه
- مسيردهی پیام‌ها در شبکه نشان گذاری میان بانک، دنا و مانا
- انجام عملیات ثبت نام دنا و مانا براساس مجوز صادر شده توسط بانک

¹ In-App

- ایجاد و تخصیص شناسه دنا به صورت منحصر بفرد برای هر دامنه فعالیت (به عبارت دیگر دنا در صورت تمایل به فعالیت در دو حوزه NFC و پرداخت درون برنامه‌ای دو شناسه منحصر بفرد از سامانه سهند دریافت می‌کند).
- انجام عملیات ثبت نام کارت در سیستم نشان گذاری به منظور صدور نشانه برای آن
- تهیه دستورالعمل فنی واسط‌های نرم افزاری برای برقراری ارتباط با دنا، مانا و بانک در پرداخت مبتنی بر نشان گذاری
- اعطای نشانه صادر شده توسط مانا به دنا
- انجام عملیات شناسایی و اعتبارسنجی در ارتباط با بانک صادر کننده 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 دنا^۱ ارسال کننده درخواست
 - سطح ۴. احراز هویت دارنده کارت به صورت خارج از کانال: ارسال رمز یکبار مصرف^۱، 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 نشان گذاری
- 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 دنا^۱ درخواست دهنده 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

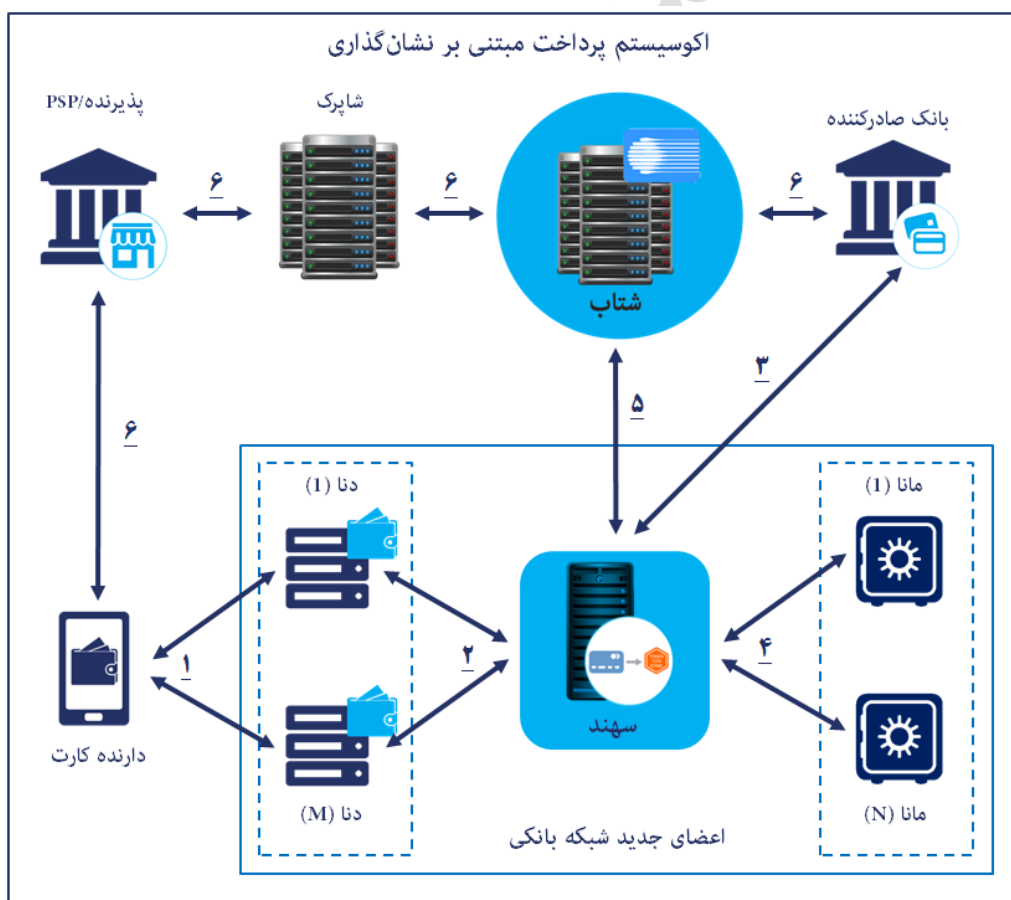
روش‌های شناسایی و اعتبارسنجی	توضیحات
بدون شناسایی و اعتبارسنجی	-
تایید اطلاعات کارت	بررسی اعتبار اطلاعات کارت اعم از شماره کارت، تاریخ انقضای کارت و CVV/CVV2
شناسایی و اعتبارسنجی مبتنی بر ریسک	ارزیابی ریسک براساس اطلاعاتی چون سابقه فعالیت کارت، موقعیت جغرافیایی دارنده کارت و سابقه دنا ارسال‌کننده درخواست
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، موقتاً غیرفعال و غیرفعال

۲- ارتباطات اعضاء اکوسیستم نشان گذاری

پس از مشخص شدن نقش‌های اکوسیستم نشان گذاری، در این بخش از مستند نحوه ارتباط اعضاء این اکوسیستم در معماری نشان گذاری 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 نشان گذاری 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 نشان گذاری 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 نشان گذاری

ارتباطات میان اعضاء سیستم پرداخت مبتنی بر نشان گذاری طبق شکل ۱ به شرح زیر می باشد:

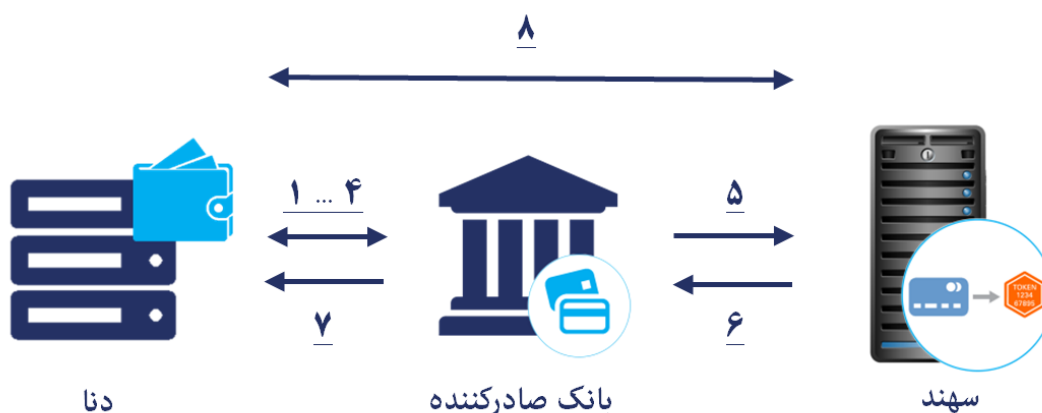
۱. ارتباط دارنده کارت با دنا:
 - درخواست ثبت شماره کارت در پرداخت مبتنی بر نشان گذاری از سوی دارنده کارت
 - اعطای نشانه از دنا به دارنده کارت
 - درخواست تغییر وضعیت نشانه
۲. ارتباط دنا با سهند:
 - ارسال درخواست ثبت شماره کارت و صدور نشانه از دنا به سهند
 - ارسال نشانه از سهند به دنا
 - ارسال درخواست 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 بازبایی 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 نشان گذاری

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

۳-۱- ثبت نام دنا در سهند

یکی از مراحل اولیه برای آغاز فعالیت های نشان گذاری، ثبت نام شرکت های مجاز برای ایفای نقش دنا است. کسب و کارهای مجازی که چنین درخواستی دارند باید مطابق شکل ۲ از طریق بانک طرف قرارداد خود طی گام های زیر اقدام به ثبت نام نمایند:



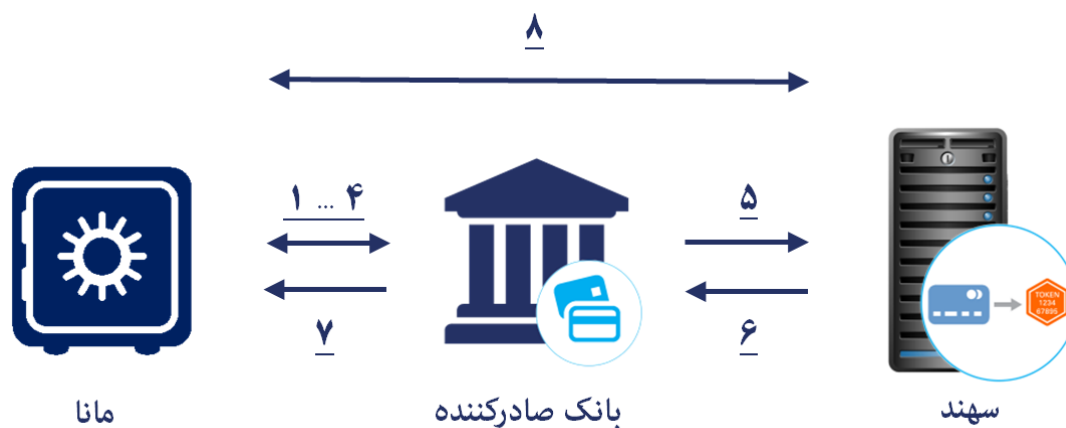
شکل ۲- فرایند ثبت نام دنا

- ۱- دنا درخواست ثبت نام را به بانک طرف قرارداد خود ارائه می دهد.
- ۲- بانک با ارائه فرم هایی به دنا، اطلاعات زیر را کسب می کند:
 - اطلاعات مرتبط با کسب و کار دنا و زمینه فعالیت آن
 - دامنه فعالیت کسب و کار دنا در حوزه نشان گذاری، اعم از فعالیت در حوزه پرداخت از طریق NFC یا پرداخت درون برنامه ای
 - نحوه ذخیره سازی اطلاعات نشانه (ذخیره سازی در برنامه کاربردی، فضای ابری و ...)
 - اسناد بالادستی مرتبط با کسب و کار دنا
- ۳- بانک الزامات تعیین شده توسط بانک مرکزی را به دنا ابلاغ می نماید.
- ۴- بانک پس از بررسی اطلاعات دریافتی و با توجه به چک لیست ها و الزاماتی که برای ممیزی امنیتی دنا در نظر گرفته شده است، صلاحیت کسب و کار آن را مورد بررسی قرار می دهد.

- ۵- در صورت تایید، بانک نام شرکت/موسسه درخواست دهنده را به اطلاع سهند رسانده و سهند شناسه منحصر بفردی را برای دنا صادر می نماید.
- ۶- سهند شناسه صادر شده را به همراه سایر اطلاعات مورد نیاز برای برقراری ارتباط میان سهند و دنا به بانک ارائه می دهد.
- ۷- بانک تأییدیه ثبت نام را به دنا اطلاع می دهد.
- ۸- ارتباط میان سهند و دنا از طریق واسط نرم افزاری ارائه شده برقرار می شود.

۳-۲- ثبت نام مانا در سهند

مانا پس از انجام موفقیت آمیز گام های زیر مطابق با شکل ۳، قادر است فعالیت خود را در حوزه نشان گذاری آغاز کند:



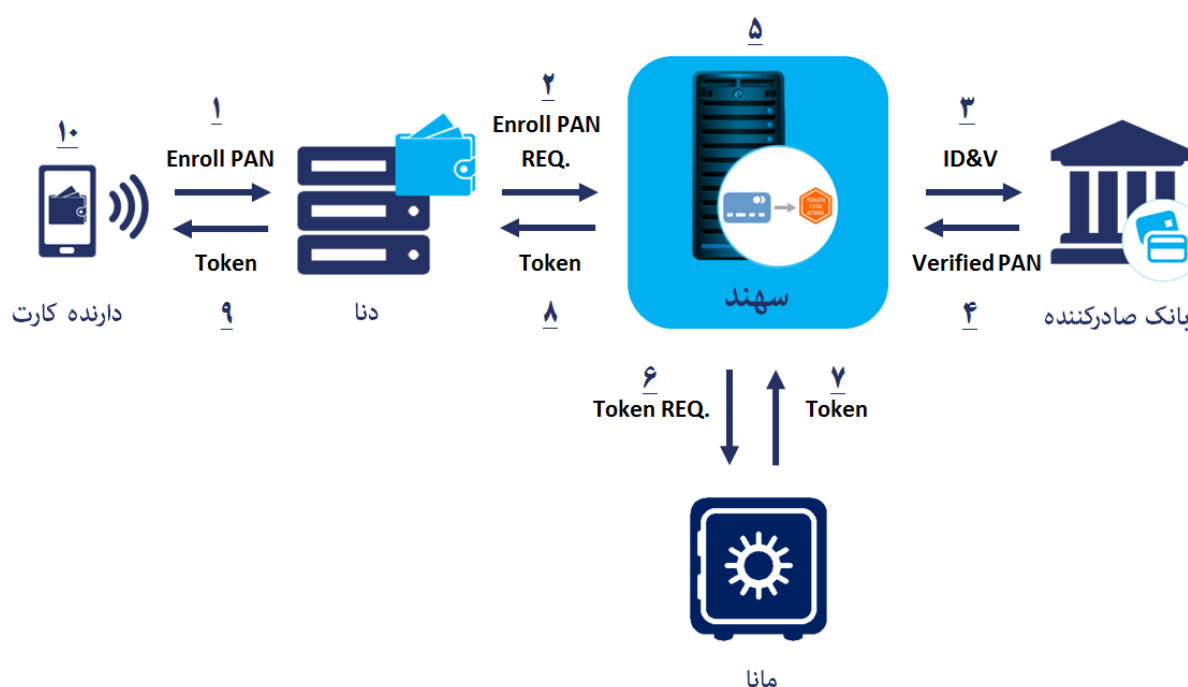
شکل ۳- فرایند ثبت نام مانا

- ۱- مانا درخواست آغاز فعالیت را به بانک طرف قرارداد خود ارائه می دهد.
- ۲- بانک الزامات تعیین شده توسط بانک مرکزی (مانند الزامات فرایندی و امنیتی نگهداری از اطلاعات کارت و نشانه) را به مانا ارائه می دهد.
- ۳- بانک با توجه به چک لیست ها 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 نرم افزاری در اختیار مانا قرار می دهد.
- ۵- بانک اطلاعات مورد نیاز برای برقراری ارتباط با مانا را در اختیار سهند قرار می دهد.

- ۶- سهند پس از انجام آزمون صحت کارکرد مانا نتیجه را در اختیار بانک قرار می دهد.
- ۷- بانک تأییدیه ثبت نام را به مانا اطلاع می دهد و محدوده مجاز شماره شناسایی بانک را که سهند برای آن بانک تعیین می نماید، به مانا اعلام می کند.
- ۸- ارتباط میان سهند و مانا از طریق واسط نرم افزاری ارائه شده برقرار می شود.

۳-۳- صدور و اعطای نشانه

در این مرحله دارنده کارت، درخواست خود برای استفاده از خدمات پرداخت مبتنی بر نشان گذاری را ارائه می دهد. عملیات صدور و اعطای نشانه به دارنده کارت طبق شکل ۴ در مراحل زیر انجام می پذیرد:



شکل ۴- فرایند صدور و اعطای نشانه

- ۱- دارنده کارت درخواست ثبت نام کارت را صادر می کند.
- ۲- دنا پس از دریافت اطلاعات از دارنده کارت، یک درخواست ثبت نام کارت به سهند ارسال می کند.
- ۳- سهند برای دریافت مجوز صدور نشانه درخواست شناسایی و اعتبارسنجی را به بانک ارسال می کند.
- ۴- بانک براساس یک یا مجموعه ای از سطوح شناسایی و اعتبارسنجی، مجوز صدور نشانه را بررسی نموده و نتیجه را به سهند ارائه می دهد.

۵- سهند بر اساس متد شناسایی و اعتبارسنجی، سطح ضمانت نشانه را تعیین می کند و برای عدم ذخیره سازی اطلاعات کارت، یک شناسه با عنوان PANUniqueReference را که برای هر کارت منحصر بفرد است تولید می کند.

۶- سهند براساس شماره شناسایی بانک، درخواست صدور نشانه را به مانای بانک صادرکننده کارت ارسال می کند.

۷- مانا برای کارت درخواست شده یک نشانه تولید می کند و تناظر میان اطلاعات کارت، PANUniqueReference، نشانه و شناسه دنا را نگهداری نموده و نشانه صادر شده را به سهند تحویل می دهد.

۸- سهند نشانه صادر شده را به همراه PANUniqueReference به دنا تحویل می دهد.

۹- دنا براساس سیاست تعیین شده در ذخیره سازی نشانه، اطلاعات زیر را ذخیره می کند:

- نشانه
- تاریخ انقضای نشانه
- کلید
- شناسه دنا

۱۰- دارنده کارت از پایان یافتن عملیات ثبت کارت در سامانه پرداخت مبتنی بر نشان گذاری توسط دنا مطلع می شود.

۳-۴- مدیریت چرخه حیات نشانه

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

- غیرفعال کردن ثبت نام در سامانه پرداخت مبتنی بر نشان گذاری
- گم/دزدیده شدن تلفن همراه
- نشت اطلاعات کارت یا نشانه
- آلوده شدن تلفن همراه به بدافزار

در هر یک از شرایط مذکور لازم است دارنده کارت براساس یکی از روش های زیر وضعیت نشانه را به روزرسانی کند:

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

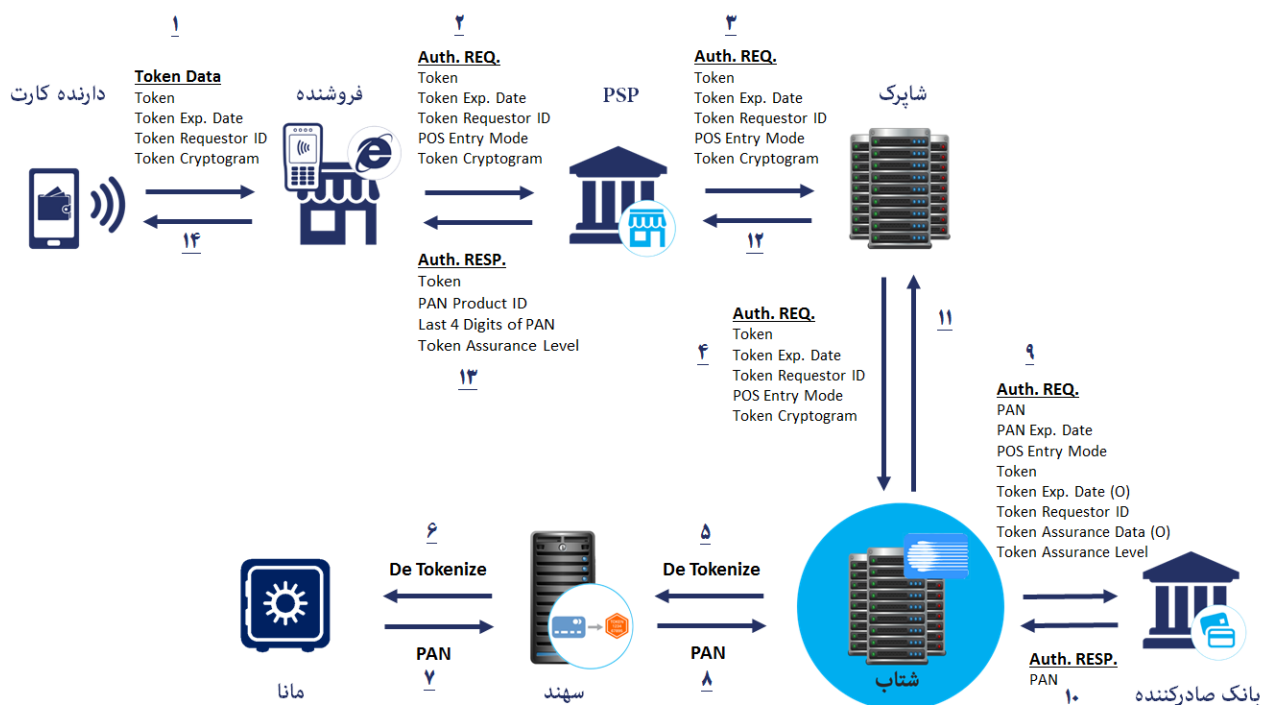
- استفاده از امکاناتی که دنا برای این منظور در نظر گرفته (به عنوان نمونه غیرفعال کردن کارت توسط کیف پول دیجیتال): دنا پیام به روزرسانی وضعیت نشانه را به سهند ارسال کرده و سهند براساس BIN نشانه، آن را به مانای مربوطه تحویل می دهد. در نهایت مانا وضعیت نشانه را به روزرسانی می نماید.

همچنین در شرایطی که دنا تقاضای به روزرسانی وضعیت نشانه های خود را داشته باشد این درخواست را به سهند ارسال کرده و سهند آن را به مانای مربوطه تحویل داده و وضعیت نشانه ها به روزرسانی می شود.

پیش نویس

۴- سناریوی پرداخت مبتنی بر نشان گذاری

در این بخش از مستند، انجام عملیات پرداخت مبتنی بر نشان گذاری در قالب سناریو شرح داده شده است. این سناریو دو نوع پرداخت از طریق NFC و پرداخت درون برنامه‌ای 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.



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

شکل ۵- سناریوی پرداخت مبتنی بر نشان گذاری

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 درون برنامه‌ای 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^۱ 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 به حداقل رسانی 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 منحصر بفرد 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 موافقی 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 پرداخت های نشان گذاری

شده با شماره نامه ۹۶/۲۷۰۶۵ م مورخ ۱۳۹۶/۲/۴

پیش نویس