بانک مرکزی جمهوری اسلامی ایران

حمایت از کالای ایرانی

باسلام؛

احتراماً، به پیوست مستند «الزامات ارائه خدمات بانکی توسط برنامک‌های همراه» ارسال می‌گردد. رعایت مفاد این مستند در برنامک همراه کلیه بانک‌ها و شرکت‌های ارائه دهنده خدمات پرداخت از ابتدای سال ۱۳۹۸ اجباری خواهد بود. شایان ذکر است ارسال تراکنش مانده‌گیری و صورتحساب توسط برنامک همراه با رعایت این الزامات، آزمون‌های موفق سامانه‌های مانا و نهاب و تطبیق با روال‌های جدید شاپرک مجاز است.
(۴۱۵۵۰۶۹)

**اداره نظام‌های پرداخت**

**داود محمدبیگی** ۲۶۱۶

**اعظم السادات آقائی پور** ۲۶۳۱-۰۳

رونوشت:

_ شرکت خدمات انفورماتیک ، مدیر محترم پروژه‌های بانک مرکزی؛ جهت اطلاع و صدور دستور مقتضی.

_ شرکت شاپرک ، مدیرعامل محترم؛ جهت اطلاع و صدور دستور مقتضی.

_ شرکت مدیریت امن الکترونیکی کاشف ، مدیرعامل محترم؛ جهت اطلاع و صدور دستور مقتضی.

بانک مرکزی جمهوری اسلامی ایران

بسمه تعالی

شماره: ۹۷/۴۳۴۳۲۷

تاریخ: ۱۳۹۷/۱۲/۰۶

پیوست: نیت حمایت از کالای ایرانی دارد

جناب آقای دکتر جلال رسول‌اف؛ مدیرعامل محترم بانک آینده

جناب آقای علیرضا بلگوری؛ مدیرعامل محترم بانک اقتصاد نوین

جناب آقای آیت‌اله ابراهیمی؛ مدیرعامل محترم بانک انصار

جناب آقای عبدالمجید پورسعید؛ مدیرعامل محترم بانک ایران زمین

رئیس محترم هیات مدیره بانک مشترک ایران - ونزوئلا

جناب آقای دکترکورش پرویزیان؛ مدیرعامل محترم بانک پارسیان

جناب آقای دکتر مجید قاسمی؛ مدیرعامل محترم بانک پاسارگاد

رئیس محترم هیات مدیره پست بانک

جناب آقای رضا دولت‌آبادی؛ مدیرعامل محترم بانک تجارت

جناب آقای حجت‌اله مهدیان‌مارانی؛ مدیرعامل محترم بانک توسعه تعاون

جناب آقای دکتر علی صالح‌آبادی؛ مدیرعامل محترم بانک توسعه صادرات ایران

جناب آقای دکتر عباس عسکرزاده؛ مدیرعامل محترم بانک حکمت ایرانیان

جناب آقای دکتر پرویز عقیلی کرمانی؛ مدیرعامل محترم بانک خاورمیانه

جناب آقای محمدرضا قربانی؛ مدیرعامل محترم بانک دی

جناب آقای دکتر محمدعلی سهمانی‌اصل؛ مدیرعامل محترم بانک رفاه کارگران

رئیس محترم هیات مدیره بانک سامان

جناب آقای محمدکاظم چقازردی؛ مدیرعامل محترم بانک سپه

جناب آقای علیرضا پویان‌شاد؛ مدیرعامل محترم بانک سرمایه

جناب آقای مهندس محمدرضا پیشرو؛ مدیرعامل محترم بانک سینا

جناب آقای احمد درخشنده؛ سرپرست محترم بانک شهر

جناب آقای دکتر حجت‌اله صیدی؛ مدیرعامل محترم بانک صادرات ایران

جناب آقای حسین مهری؛ مدیرعامل محترم بانک صنعت و معدن

جناب آقای محمدحسین حسین‌زاده؛ مدیرعامل محترم بانک قرض‌الحسنه‌رسالت

جناب آقای دکتر مرتضی اکبری؛ مدیرعامل محترم بانک قرض‌الحسنه‌مهرایران

جناب آقای غلامحسین تقی‌نتاج‌ملکشاه؛ مدیرعامل محترم بانک قوامین

جناب آقای حمید تهرانفر؛ مدیرعامل محترم بانک کارآفرین

جناب آقای روح‌اله خدارحمی؛ مدیرعامل محترم بانک کشاورزی

جناب آقای مرتضی خامی؛ مدیرعامل محترم بانک گردشگری

جناب آقای ابوالقاسم رحیمی انارکی؛ مدیرعامل محترم بانک مسکن

جناب آقای محمد بیگدلی؛ مدیرعامل محترم بانک ملت

جناب آقای محمدرضا حسین‌زاده؛ مدیرعامل محترم بانک ملی ایران

رئیس محترم هیات مدیره موسسه اعتباری توسعه

جناب آقای جواد فهیمی‌پور؛ قائم‌مقام محترم مدیرعامل موسسه اعتباری کوثر

جناب آقای سیدامین جوادی؛ مدیرعامل محترم موسسه اعتباری ملل

رئیس محترم هیات مدیره موسسه اعتباری نور

بانک مرکزی جمهوری اسلامی ایران

معاونت فن‌آوری‌های نوین

اداره نظام‌های پرداخت

# مستند الزامات ارائه خدمات بانکی توسط برنامک‌های همراه

---

CBI-Regulation-PSApp-v3.2

زمستان ۱۳۹۷

ارائه انواع خدمات مبتنی بر کارت‌های بانکی در برنامک‌های همراه[1]، منوط به رعایت کامل موارد به شرح ذیل توسط بانک‌ها، موسسات مالی و اعتباری و شرکت‌های ارائه‌دهنده خدمات پرداخت[2] است که از این پس با عنوان موسسه از آنها یاد خواهد شد:

۱- موسسه موظف است ضمن رعایت ملاحظات امنیتی و طی انجام فرایندهای تست و ارزیابی امنیتی، از امن بودن برنامک همراه اطمینان حاصل نماید. مسئولیت وقوع هرگونه رخداد امنیتی، تقلب و کلاهبرداری، سوءاستفاده از اطلاعات شخصی و مالی کاربران برنامک همراه مستقیماً به عهده موسسه مربوطه است.

۲- موسسه موظف است هنگام فعال‌سازی برنامک همراه بر روی دستگاه کاربر، اقدامات زیر را انجام دهد:

- کد ملی و شماره تلفن همراه کاربر را اخذ نماید.
- تطابق کد ملی با شماره تلفن همراه اظهار شده توسط کاربر را از طریق سامانه نهاب استعلام نماید.
- با ارسال پیامک حاوی کد اعتبارسنجی یکبار مصرف به شماره تلفن همراه تایید شده توسط سامانه نهاب، اطمینان حاصل نماید که سیم کارت معرفی شده در اختیار کاربر اظهارکننده آن است.
- سوابق مرتبط با فعال‌سازی‌های موفق و ناموفق را به مدت حداقل یکسال ثبت و نگهداری نماید.

۳- موسسه موظف است هنگام ثبت و فعال‌سازی کارت بانکی در برنامک همراه اقدامات زیر را انجام دهد:

- ابتدا از انجام موفقیت‌آمیز فعال‌سازی برنامک همراه مطابق با بند ۲ این بخشنامه اطمینان حاصل نماید.
- طی فرایند ارائه شده در مستند «راهنمای کاربری سرویس برخط مانا»، تطابق شماره کارت، کد ملی و شماره تلفن همراه از سامانه مانا را استعلام نموده و نشانه مربوط به کارت را اخذ نماید.
- به ازای هر برنامک همراه فعال‌سازی شده، یک شناسه یکتا، تصادفی و غیرقابل پیش‌بینی (به نام PaymentAppInstanceID)[3] تولید و به سامانه مانا ارسال کند.
- نشانه مربوط به هر کارت نبایستی توسط کاربر قابل مشاهده باشد.
- در صورت نیاز کاربر به کسب اطلاع از شماره کارت خود در برنامک این شماره به صورت نهان‌شده[4] قابل نمایش است به گونه‌ای که ۶ رقم اول و ۴ رقم آخر شماره کارت قابل مشاهده و سایر ارقام با کاراکتر * نشان داده شود.

۴- لازم است برای هر کارت بانکی در هر برنامک همراه صرفاً یک نشانه صادر شده و نشانه توسط برنامک همراه از سامانه مرکزی موسسه مربوطه فراخوانی شود.

۵- نشانه صادر شده براساس تجهیزی (اعم از تلفن همراه و تبلت) که درخواست فعال‌سازی از طریق آن ارسال شده، مجزا خواهد بود. به عنوان نمونه در صورت فعال‌سازی کارت بانکی از طریق دو تجهیز، دو نشانه متفاوت صادر می‌گردد.

- لازم است پیش از انجام تراکنش، تطابق میان نشانه و شناسه یکتا (PaymentAppInstanceID) توسط موسسه انجام شود، سپس در صورت مطابقت نشانه و شناسه یکتا، تراکنش ایجاد گردد و در غیر این صورت از ایجاد تراکنش ممانعت به عمل آید.

---

[1] منظور از برنامک همراه در این مستند، هر نوع برنامک همراه متعلق به بانک، موسسه اعتباری یا شرکت ارائه دهنده خدمات پرداخت که به نحوی خدمات بانکی یا پرداخت را به کاربران ارائه می‌دهد.

[2] PSP

[3] هدف از تولید این شناسه، در اختیار داشتن داده‌ای منحصربفرد از برنامک همراه برای مقاصد کنترلی است.

[4] Masked

۶- موسسه موظف است کاربر را در هر بار ورود به برنامک همراه برای استفاده از خدمات بانکی، از طریق سازوکارهایی نظیر نام کاربری و گذرواژه، تشخیص چهره و نظایر آن بنابر طراحی برنامک شناسایی نماید.

۷- لازم است کلیه خدمات بانکی، صرفاً در صورت تطابق کد ملی اخذ شده در مرحله فعال‌سازی برنامک همراه و کد ملی دارنده کارت بانکی ارائه گردد.

۸- لازم است کانال ارتباطی میان موسسه و برنامک همراه، دارای رمزنگاری End-to-End باشد و در هیچ‌یک از سازوکارهای مبتنی بر رمزنگاری از الگوریتم‌های رمزنگاری ضعیف و غیراستاندارد استفاده نشود.

۹- شرکت ارائه‌دهنده خدمات پرداخت تحت هیچ شرایطی نباید شماره کارت، کد CVV2، رمز دوم کارت و اطلاعات مالی مشتریان نظیر مانده حساب و صورتحساب آنها را در سامانه‌های خود اعم از سامانه مرکزی و برنامک همراه ذخیره نماید.

۱۰-ارائه تمامی خدمات کارتی در برنامک همراه صرفاً با استفاده از نشانه ارائه شده توسط سامانه مانا مجاز است.

۱۱-موسسه موظف است برای هر یک از برنامک‌های همراه به طور جداگانه اقدام به انجام آزمون اتصال به سامانه مانا نماید و هریک از برنامک‌های همراه صرفاً در صورت موفقیت‌آمیز بودن عملیات آزمون سامانه مانا، مجاز به ارائه خدمات کارتی خواهند بود.

۱۲-لازم است در موارد زیر فرایند اطلاع‌رسانی به کاربر توسط موسسه انجام شود:

- فعال‌سازی برنامک همراه از طریق پیامک
- فعال‌سازی کارت بانکی در برنامک همراه از طریق پیامک
- معرفی شرایط و مقررات[۵] خدمات بانکی مورد استفاده در برنامک همراه و اخذ تاییدیه کاربر پیش از فعال‌سازی

۱۳-لازم است به منظور پاسخگویی به نهادهای ذیصلاح قابلیت انجام اقدامات زیر توسط موسسه فراهم گردد:

- دریافت کد ملی و شماره تلفن همراه کاربر از طریق شناسه یکتا یا نشانه
- امکان حذف یا مسدودسازی نشانه از طریق سامانه مرکزی موسسه

۱۴-لازم است در صورت درخواست کاربر، امکان حذف، غیرفعال‌سازی نشانه در برنامک همراه فراهم شود.

۱۵-لازم است هرگونه تغییر اعلامی در سامانه مانا شامل ارائه نسخه جدید از یک سرویس یا ارائه یک سرویس جدید، ظرف مدت یک ماه توسط موسسه پیاده‌سازی شود و در صورت عدم پیاده‌سازی، دسترسی‌های آنها حذف خواهد شد.

۱۶-لازم است موسسه اطلاعاتی از برنامک همراه و تراکنش‌های صادرشده توسط آن را به نحوی در سامانه مرکزی خود ثبت و نگهداری نماید که امکان رهگیری تمامی عملیات تراکنشی برنامک همراه، فعال‌سازی برنامک و فعال‌سازی کارت فراهم گردد.

۱۷-لازم است فرایند دریافت برنامک همراه فقط از طریق درگاه‌های معتبر و اصیل مربوط به موسسه به‌صورت امن مقدور باشد، به نحوی که اثبات اصالت توزیع برنامک همراه برای مراجع ذیصلاح امکان‌پذیر باشد.

۱۸-شرکت‌های ارائه‌دهنده خدمات پرداخت موظفند از اطلاعاتی که از کاربر برنامک همراه گردآوری شده صرفاً در خدمات موضوع این بخشنامه بهره‌برداری نمایند. استفاده از این اطلاعات برای سایر مقاصد تجاری و کسب‌وکاری غیرمجاز محسوب می‌شود.

در صورت عدم رعایت موارد فوق و ارائه هرگونه خدمات در این خصوص، موارد شناسایی شده به عنوان موارد مشکوک به مراجع مربوطه ارجاع خواهد شد.

---

[۵] Term and Conditions