بانک مرکزی جمهوری اسلامی ایران

اداره نظام های پرداخت

الزامات امنیتی فضای تولید و تبادل اطلاعات بانکی

الزامات رمزهای پویا
در تراکنش‌های مبتنی بر کارت

BIS RG 300-14

شهریور ۱۳۹۷

شناسنامه

۱. اعتباربخشی

بر اساس بند ۱۰-۱ از «سند راهبردی مدیریت امنیت اطلاعات» در حوزه بانک‌ها و مؤسسات اعتباری، مصوب خردادماه ۱۳۸۸، تهیه برنامه‌ها و دستورالعمل‌های اجرایی مربوط به سند پیش‌گفته بر عهده بانک مرکزی قرار داده شده است. همچنین بانک مرکزی ج.ا.ا باهدف پایش و کنترل امنیت فضای تولید و تبادل اطلاعات بانکی و بر اساس مصوبه یک هزار و یک‌صد و پنجاه و یکمین جلسه شورای پول و اعتبار، مرکز کاشف را ایجاد کرده و مسئولیت تنظیم مقررات و الزامات امنیت اطلاعات را به‌موجب «بند یکم ماده دوم مقررات ناظر بر فعالیت مرکز کاشف» مبنی بر «تدوین و تعیین اهداف، سیاست‌های کلان، راهبردها و الزامات امنیت اطلاعات» به آن مرکز واگذار نموده است. بر همین اساس بانک مرکزی ج.ا.ا وظیفه تنظیم و نگهداری الزامات «رمزهای پویا در تراکنش‌های مبتنی بر کارت» را بر عهده مرکز کاشف نهاده است.

همچنین بر اساس «بند دوم ماده دوم مقررات ناظر بر فعالیت مرکز کاشف» مبنی بر «نظارت بر حسن اجرای سیاست‌های کلان، راهبردها و الزامات امنیت اطلاعات»، نظارت بر حسن اجرای الزامات «رمزهای پویا در تراکنش‌های مبتنی بر کارت» نیز توسط ناظران مرکز کاشف انجام خواهد شد.

سند حاضر بر اساس «ماده هشتم مقررات ناظر بر فعالیت مرکز کاشف» توسط شرکت مدیریت امن الکترونیکی کاشف که به نمایندگی از بانک مرکزی ج.ا.ا مسئولیت ایجاد، راهبری و اجرای وظایف محول شده به «مرکز کاشف» را بر عهده دارد، تهیه و تدوین شده است.

۲. عنوان الزامات

«رمزهای پویا در تراکنش‌های مبتنی بر کارت»

۳. طبقه الزامات

«امنیت خدمات و فناوری‌های بانکی و پرداخت»

۴. توضیحات

این سند بیان‌کننده حداقل الزاماتی است که بانک‌ها و مؤسسات اعتباری باید در خصوص استفاده از رمزهای پویا به‌عنوان رمزهای مرتبط با کارت‌های بانکی رعایت کنند.

۵. نهاد تصویب‌کننده

بانک مرکزی جمهوری اسلامی ایران

۶. مسئول نگهداری و به‌روزرسانی

مسئولیت نگهداری و به‌روزرسانی الزامات «رمزهای پویا در تراکنش‌های مبتنی بر کارت» بر عهدهٔ شرکت کاشف است.

۷. کاربردپذیری

الزامات «رمزهای پویا در تراکنش‌های مبتنی بر کارت» در تمامی بانک‌ها و مؤسسات اعتباری که به موجب قانون یا با مجوز بانک مرکزی تأسیس‌شده و تحت نظارت بانک مرکزی هستند، کاربردپذیر است. سند حاضر دارای حق استفاده انحصاری در بانک‌ها و مؤسسات اعتباری نبوده و می‌تواند بخش یا بخش‌هایی از آن در نهادهای فعال در شبکه پرداخت کارتی یا بازار غیرمتشکل پولی کشور به‌صورت داوطلبانه مورداستفاده قرار گیرد.

۸. اجرا

الزامات «رمزهای پویا در تراکنش‌های مبتنی بر کارت» با سایر الزامات کاربردپذیر در نظام بانکی کشور سازگاری داشته و امکان مخالفت یا رد بخش یا بخش‌هایی از دیگر قوانین، مقررات، الزامات یا استانداردهای حاکم بر نظام بانکی به‌واسطهٔ تفسیر/استناد جزئی یا کلی از/به این سند، وجود ندارد.

پیاده‌سازی الزامات «رمزهای پویا در تراکنش‌های مبتنی بر کارت» نافی مسئولیت‌ها و پاسخگویی بانک‌ها و مؤسسات اعتباری درخصوص مدیریت مخاطرات خدمات مبتنی بر کارت‌های بانکی نیست.

۹. زمان‌بندی اجرا و نظارت

الزامات «رمزهای پویا در تراکنش‌های مبتنی بر کارت» از تاریخ ابلاغ بانک مرکزی ج.ا.ا قابلیت پیاده‌سازی و اجرایی شدن توسط بانک‌ها و مؤسسات اعتباری را دارد.

۱۰. قوانین، مقررات و اسناد مرتبط

- «الزامات بهره‌برداری امن از دستگاه‌های خودپرداز» (BIS RG 300-10)، بخشنامه شماره ۹۵/۴۱۷۷۳۰ مورخ ۱۳۹۵/۱۲/۲۵
- «الزامات امنیتی مرتبط با رمزهای کارت»، بخشنامه شماره ۹۵/۴۱۸۳۲۱ مورخ ۱۳۹۵/۱۲/۲۵
- «الزامات گزارش دهی رخدادهای امنیت اطلاعات بانکی» (BIS RG 200-10)، بخشنامه شماره ۹۷/۴۹۴۸۸ مورخ ۱۳۹۷/۰۲/۲۰

۱۱. نحوه دسترسی

الزامات «رمزهای پویا در تراکنش‌های مبتنی بر کارت» از طریق پورتال اطلاع‌رسانی اداره نظام‌های پرداخت بانک مرکزی ج.ا.ا در دسترس است.

۱۲. تصویب و ابلاغ

الزامات «رمزهای پویا در تراکنش‌های مبتنی بر کارت» مشتمل بر دو بخش، پنجاه‌وهشت ماده و هشت تبصره در تاریخ ۹۷/۰۶/۰۱ تصویب و ابلاغ گردید.

فهرست مطالب

بخش یکم-کلیات

مبحث یکم- تعاریف

ماده ۱) تعاریف و قراردادهای به‌کاررفته در سند حاضر به شرح ذیل‌اند:

الف) مؤسسه اعتباری: بانک یا مؤسسه اعتباری غیر بانکی است که به‌موجب قانون یا با مجوز بانک مرکزی تأسیس‌شده و تحت نظارت بانک مرکزی است.

ب) رمز اول کارت: رمز مورداستفاده توسط دارنده کارت بانکی به‌منظور بهره‌گیری از خدمات با حضور فیزیکی کارت مانند خرید با استفاده از پایانه‌های فروش و دریافت وجه با استفاده از دستگاه‌های خودپرداز.

ج) رمز دوم کارت: رمز مورداستفاده توسط دارنده کارت بانکی به‌منظور بهره‌گیری از خدمات بدون نیاز به حضور فیزیکی کارت مانند خرید اینترنتی با استفاده از درگاه‌های پرداخت اینترنتی.

د) رمز پویا: رمز اول یا دوم کارت که متغیر بوده و پذیرش آن توسط مؤسسه اعتباری در خدمات بانکداری و پرداخت الکترونیکی مبتنی بر کارت در یک بازه زمانی مشخص، تنها یک‌بار صورت پذیرد.

هـ) مهندسی اجتماعی: تلاش برای فریب افراد و ترغیب آنها به افشای اطلاعات حساس نظیر گذرواژه‌ها یا ترغیب آنها به انجام یک عمل خاص مانند انتقال وجه به حساب کلاه‌برداران، با استفاده از ابزارهای رایانه‌ای یا غیررایانه‌ای.

و) احراز هویت: رویه‌ای است که از طریق آن مؤسسه اعتباری، هویت دارنده کارت بانکی را تصدیق کرده یا استفاده از ابزار پرداخت مشخصی را اعتباربخشی می‌کند.

ز) عناصر احراز هویت: عناصری در دسته‌های دانستنی[1] (آنچه تنها کاربر می‌داند) مانند رمز، داشتنی[2] (آنچه تنها کاربر دارد) مانند توکن سخت‌افزاری و ویژگی ذاتی[3] (آنچه کاربر هست) مانند اثرانگشت.

ح) احراز هویت چندعاملی: احراز هویتی مبتنی بر به‌کارگیری دو یا چند عنصر از عناصر احراز هویت است.

ط) افزاره ارائه رمزهای پویا: هرگونه ابزاری اعم از مؤلفه‌های نرم‌افزاری طراحی‌شده برای دستگاه‌های چندمنظوره[4] یا دستگاه‌های خاص‌منظوره مانند توکن‌های سخت‌افزاری که مؤسسه اعتباری به‌منظور ارائه رمزهای پویا در اختیار دارنده کارت بانکی قرار می‌دهد. در فرآیند احراز هویت دارندگان کارت در خدمات مبتنی بر کارت، افزاره ارائه‌دهنده رمز پویا آن چیزی است که دارنده کارت در اختیار دارد (داشتنی).

ی) نانس[5]: مقداری است که در الگوریتم‌های تولید رمز پویا، برای محاسبه رمز پویا از آن استفاده می‌شود. این مقدار مبتنی بر زمان یا شمارشگر یا ترکیبی از آن دو است.

ک) کلید محرمانه تولید رمز پویا: کلید متقارنی است که برای افزاره ارائه‌دهنده رمز پویای مشخصی به‌صورت مادام‌العمر ثابت بوده و پس از ترکیب با نانس در یک الگوریتم امن منجر به تولید رمز پویا می‌شود.

ل) کانال از راه دور: کانالی است برای تعامل دارنده کارت بانکی و مؤسسه اعتباری به‌نحوی‌که در آن کانال، نیازی به حضور فیزیکی دارنده کارت در محلی مشخص (مانند شعبه، پایانه فروش یا دستگاه خودپرداز) ندارد و این تعامل از طریق شبکه اینترنت یا با استفاده از ابزارهای مورداستفاده برای ارتباطات از راه دور، انجام می‌شود.

---

[1] Knowledge
[2] Possession
[3] Inherence

[4] نظیر تلفن همراه، رایانک و غیره

[5] Nonce

م) **کانال محافظت‌شده:** کانال ارتباطی رمز شده‌ای که از استانداردهای رمزنگاری مطمئن استفاده کرده و در آن آغازگر ارتباط (کارخواه[6])، هویت پذیرنده ارتباط (کارگزار[7]) را تصدیق نموده است. کانال ارتباطی محافظت‌شده، محرمانگی اطلاعات مبادله شده در کانال را تضمین کرده و در برابر حملاتی نظیر SIM Swap و MitM[8] مقاوم است.

مبحث دوم- هدف

ماده ۲) هدف از این مقررات، ارائه الزاماتی به‌منظور حصول اطمینان مؤسسات اعتباری صادرکننده کارت‌های بانکی، از کاهش مخاطرات ایستا بودن رمزهای کارت‌های بانکی است.

مبحث سوم- محدوده

ماده ۳) این سند به بیان حداقل الزامات استفاده از رمزهای پویا به‌عنوان رمزهای مرتبط با کارت‌های بانکی می‌پردازد.

تبصره) الزامات مندرج در سند حاضر شامل حداقل‌های موردنیاز جهت ارائه خدمت رمزهای پویاست و مؤسسه اعتباری بایستی در صورت لزوم و بر اساس نتایج ارزیابی مخاطره انجام‌شده، کنترل‌های امنیتی تکمیلی را به‌منظور مقابله با مخاطرات احصاء شده، تعیین نماید و به کار بندد.

بخش دوم – الزامات خدمت رمزهای پویا

مبحث چهارم- الزامات عمومی

ماده ۴) مؤسسه اعتباری باید اطمینان حاصل کند که «رمز دوم» کارت‌های صادرشده توسط آن مؤسسه، رمز پویا و منطبق با الزامات مندرج در سند حاضر است.

تبصره) توصیه می‌شود مؤسسه اعتباری در خصوص تراکنش‌های «با مخاطره زیاد» در خدماتی که از «رمز اول» کارت‌های بانکی استفاده می‌کنند، از رمز پویا با مشخصات مندرج در این سند، به‌جای رمز اول استفاده کند.

ماده ۵) مؤسسه اعتباری باید با اتخاذ اقدامات امنیتی لازم، از محرمانگی، صحت و تمامیت رمزهای پویا در تمامی مراحل تولید، انتقال و به‌کارگیری حصول اطمینان نماید.

ماده ۶) در سازوکارهای مبتنی بر رمزنگاری، تمامی فرآیندهای مدیریت اجزای محرمانه رمزنگاری، شامل تولید، توزیع، نگهداری، جایگزینی و امحاء در سمت دارنده کارت و مؤسسه اعتباری باید منطبق با استانداردها و به‌روش‌های امنیتی مدیریت کلید باشد.

ماده ۷) در هیچ‌یک از سازوکارهای مبتنی بر رمزنگاری نباید از الگوریتم‌های رمزنگاری ضعیف (نظیر SHA1، DES، MD5) و غیراستاندارد استفاده شود.

ماده ۸) مؤسسه اعتباری باید با اتخاذ تمهیدات لازم، مخاطرات مرتبط با مهندسی اجتماعی و فریب دارندگان کارت‌های بانکی توسط کلاه‌برداران – برای سوءاستفاده از رمزهای پویا – را کاهش دهد.

[6] Client
[7] Server
[8] Man-in-the-Middle

راهنما: مؤسسه اعتباری می‌تواند به‌صورت مستمر و با انتخاب روش‌های اثربخش، دارندگان کارت بانکی را از نحوه حفاظت از رمزهای پویا آگاه نموده و آنها را نسبت به شگردهای مورداستفاده کلاه‌برداران برای دسترسی غیرمجاز به رمزهای پویا آگاه نماید.

ماده ۹) مؤسسه اعتباری باید پس از حداکثر پنج تلاش ناموفق متوالی برای ورود رمز پویا، در یک مدت‌زمان معین، ارائه خدمت مرتبط را به دارنده کارت، به‌طور موقت یا دائم مسدود کند.

تبصره ۱) زمانی که مسدودسازی موقتی باشد، مدت‌زمان مسدودی و تعداد دفعات مسدودی را باید بر اساس ویژگی‌های خدمت ارائه‌شده به دارنده کارت بانکی و مخاطرات مرتبط با آن تعیین کرد.

تبصره ۲) مؤسسه اعتباری باید پیش از مسدودسازی دائم خدمت، دارنده کارت بانکی را مطلع نماید.

ماده ۱۰) زمانی که مسدودسازی دائمی باشد، باید رویه‌ای امن ایجاد شود تا دارنده کارت بانکی بتواند استفاده از خدمات بانکداری و پرداخت الکترونیکی مسدود شده را از سر گیرد.

ماده ۱۱) مؤسسه اعتباری باید فرآیندها و نحوه پیاده‌سازی الزامات مندرج در این سند را به‌طور کامل مستند نموده و بنا به درخواست در اختیار بانک مرکزی ج.ا.ا قرار دهد.

مبحث پنجم- مشخصات رمز پویا

ماده ۱۲) حداقل طول رمز پویای جایگزین رمز اول کارت باید چهار رقم باشد.

ماده ۱۳) حداقل طول رمز پویای جایگزین رمز دوم کارت باید هفت رقم باشد.

ماده ۱۴) طول عمر رمزهای پویا باید حداکثر شصت ثانیه بوده و پس از این زمان رمز تولیدشده منقضی و غیرقابل استفاده شود.

ماده ۱۵) رمزهای پویا در طول عمر خود، باید تنها یک‌بار توسط مؤسسه اعتباری پذیرفته شوند.

ماده ۱۶) رمزهای پویا باید در طول عمر خود صرفاً برای استفاده از خدمات مبتنی بر «یک کارت مشخص» -از بین کارت‌های صادرشده توسط مؤسسه اعتباری- قابل‌استفاده باشند.

مبحث ششم-ثبت‌نام برای استفاده از خدمت رمزهای پویا

ماده ۱۷) استفاده از خدمت رمزهای پویا و جایگزینی آنها به‌جای رمزهای ایستا در خدمات مبتنی بر کارت، نیازمند ثبت‌نام دارندگان کارت بانکی است.

ماده ۱۸) ثبت‌نام حضوری برای استفاده از رمزهای پویا در محل شعب مؤسسه اعتباری، منوط به احراز هویت مطمئن (کنترل مدارک هویتی و استعلام از سامانه ثبت‌احوال) دارنده کارت بانکی است.

ماده ۱۹) ثبت‌نام حضوری برای استفاده از رمزهای پویا از طریق دستگاه‌های خودپرداز، منوط به احراز هویت مطمئن مشتری بر پایه حضور کارت، ورود رمز اول و تائید کد احراز هویت ارسال شده به شماره تلفن همراه دارنده کارت (به‌عنوان یکی از عوامل احراز هویت)، از سوی بانک است.

تبصره) ثبت‌نام از طریق دستگاه‌های خودپرداز تنها روی دستگاه‌هایی مجاز است که متعلق به مؤسسه اعتباری صادرکننده کارت بوده و منطبق با «الزامات بهره‌برداری امن از دستگاه‌های خودپرداز» (BIS RG 300-10) باشند.

ماده ۲۰) ثبت‌نام غیرحضوری برای استفاده از رمزهای پویا از طریق شبکه اینترنت یا کانال‌های ارتباطی راه دور، بایستی متکی بر احراز هویت چندعاملی باشد.

ماده ۲۱) مؤسسه اعتباری تنها زمانی می‌تواند از شماره تلفن همراه به‌عنوان یکی از عوامل احراز هویت استفاده کند که از تطابق اطلاعات مالک شماره تلفن همراه با اطلاعات دارنده کارت اطمینان یابد.

ماده ۲۲) مؤسسه اعتباری باید امکان غیرفعال کردن خدمت رمزهای پویا را برای دارندگان کارت بانکی مطابق بند ۱-۶ از بخشنامه شماره ۹۵/۴۱۸۳۲۱ فراهم نماید.

راهنما: منظور از غیر فعال کردن خدمت، حذف استفاده از خدمات مرتبط با رمز دوم کارت است.

ماده ۲۳) مؤسسه اعتباری باید اطمینان یابد که تجدید و فعال‌سازی مجدد خدمت رمزهای پویا، با الزامات مندرج در مبحث ششم انطباق دارد.

ماده ۲۴) مؤسسه اعتباری باید سازوکاری را فراهم نماید تا در صورت تغییر دستگاه چندمنظوره یا شماره تلفن همراه دارنده کارت، ادامه ارائه خدمت رمز پویا به دارنده کارت، منوط به ثبت‌نام مجدد (مطابق مفاد مندرج در مبحث ششم) باشد.

مبحث هفتم- تولید رمز پویا

ماده ۲۵) مؤسسه اعتباری باید در تولید رمزهای پویا از استانداردهای شناخته‌شده استفاده نماید.

راهنما: برای تولید OTP بر اساس HOTP (HMAC-based One-time Password) و TOTP (Time-based One-time Password) می‌توان از سازوکارهای تشریح شده در RFC های 4226 و 6238 استفاده کرد.

ماده ۲۶) حداقل طول کلید محرمانه مورداستفاده برای تولید رمزهای پویا باید ۱۱۲ بیت باشد.

ماده ۲۷) طول نانس مورداستفاده برای تولید رمز پویا باید به‌اندازه‌ای باشد که مؤسسه اعتباری از «یکتا» ماندن آن در هر عملیات و در تمام طول عمرش اطمینان یابد.

ماده ۲۸) نباید امکان تولید رمز پویای جدید بر اساس هیچ‌یک از رمزهای پویای پیش‌تر تولیدشده، وجود داشته باشد.

ماده ۲۹) با افشای یک رمز پویا، نباید هیچ‌گونه اطلاعاتی از عوامل احراز هویت، قابل‌استخراج باشد.

مبحث هشتم- انتقال اطلاعات حساس

ماده ۳۰) توزیع کلیدهای محرمانه مورداستفاده برای تولید رمزهای پویا باید از طریق کانال محافظت‌شده انجام پذیرد.

ماده ۳۱) مؤسسه اعتباری برای دریافت/ارسال رمزهای پویا از/به دارندگان کارت بانکی باید از کانال‌های محافظت‌شده که در مقابل استراق سمع و حملاتی نظیر SIM Swap و MitM مقاوم هستند، استفاده نماید.

مبحث نهم- الزامات افزاره‌های ارائه رمز پویا

ماده ۳۲) مؤسسه اعتباری می‌تواند از افزاره‌های نرم‌افزاری یا دستگاه‌های خاص‌منظوره مانند توکن‌های سخت‌افزاری برای ارائه رمزهای پویا به دارندگان کارت بانکی استفاده کند.

ماده ۳۳) مؤسسه اعتباری باید اطمینان یابد که افزاره‌های ارائه رمز پویا به شیوه‌ای امن به دارنده کارت بانکی ارتباط داده‌شده است.

ماده ۳۴) مؤسسه اعتباری باید اطمینان یابد که افزاره ارائه رمز پویا در مالکیت و کنترل دارنده کارت بانکی قرار دارند.

تبصره) مؤسسه اعتباری باید دارنده کارت را از مخاطرات جابه‌جایی شماره تلفن همراه آگاه سازد.

ماده ۳۵) استفاده هم‌زمان از چند افزاره ارائه رمزهای پویا برای یک کارت بانکی غیرمجاز است.

ماده ۳۶) افزاره ارائه رمز پویا –به‌ویژه افزاره‌های مبتنی بر نرم‌افزار– باید از استخراج و کپی شدن کلید محرمانه تولید رمزهای پویا و استفاده از آنها در افزاره‌های دیگر جلوگیری به عمل آورد.

ماده ۳۷) هرگونه استفاده از افزاره ارائه رمز پویا باید مستلزم ورود حداقل یک عامل احراز هویت دیگر از نوع دانستنی (آنچه تنها دارنده کارت می‌داند)، یا ویژگی ذاتی (مانند مشخصه زیست‌سنجی از دارنده کارت) باشد.

راهنما: عوامل احراز هویت دانستنی یا ویژگی ذاتی، ممکن است از طریق یک صفحه‌کلید یا یک خوانشگر زیست‌سنجه[9] که با افزاره ارائه‌دهنده رمز پویا یکپارچه‌شده، دریافت شود.

ماده ۳۸) درصورتی‌که عامل احراز هویت به کار گرفته شده برای استفاده از افزاره ارائه‌دهنده رمز پویا از نوع «دانستنی» باشد، باید حداقل الزامات زیر برآورده شوند:

الف) حداقل طول عامل دانستنی در افزاره‌های خاص‌منظوره سخت‌افزاری معادل چهار رقم باشد.

ب) حداقل طول عامل دانستنی در افزاره‌های نرم‌افزاری معادل هشت کاراکتر باشد.

ج) در افزاره‌های نرم‌افزاری نباید از قابلیت «یادآور گذرواژه[10]» استفاده کرد.

د) در افزاره‌های نرم‌افزاری نباید از قابلیت «پرسش‌های امنیتی» استفاده کرد.

هـ) هنگام انتخاب یا تغییر رمز در افزاره‌های نرم‌افزاری، از انتخاب رمزهای رایج یا پرمخاطره جلوگیری گردد.

و) شمار تلاش‌های ناموفق متوالی نباید بیش از پنج بار شود. به‌محض رسیدن به حدود مزبور، باید اقدامات ذیل انجام پذیرد:

- ایجاد وقفه زمانی حداقل سی ثانیه‌ای پیش از تلاش بعدی و افزایش زمان وقفه‌های بعدی به‌صورت نمایی (برای نمونه: یک دقیقه وقفه پس از تلاش ناموفق اول، دو دقیقه وقفه پس از تلاش ناموفق دوم و به همین ترتیب . . .) یا
- توقف فرآیند دریافت عامل دانستنی از دارنده افزاره ارائه‌دهنده رمز پویا و پیشنهاد عاملی دیگر جهت احراز هویت (برای نمونه: شرط زیست‌سنجی یا گذرواژه دیگر، درصورتی‌که چنین روش جایگزینی از قبل تعریف شده باشد)

ز) چنانچه شواهدی از لو رفتگی عامل دانستنی وجود داشته باشد، باید دارنده کارت را وادار نمود تا رمز خود را تغییر دهد.

ح) هنگام واردکردن عامل دانستنی، کاراکترهای ورودی به‌صورت ناخوانا نمایش داده شود.

ط) عامل دانستنی باید به شکلی ذخیره شود که امکان تغییر و بازیابی آن توسط افراد غیرمجاز وجود نداشته باشد.

ماده ۳۹) درصورتی‌که عامل احراز هویت به کار گرفته شده برای استفاده از افزاره ارائه‌دهنده رمز پویا از نوع «ویژگی ذاتی» باشد، باید حداقل الزامات زیر برآورده شوند:

الف) ویژگی ذاتی از طریق یک حس‌گر فیزیکی دریافت شود.

ب) سازوکار زیست‌سنجی تا حد امکان در برابر ویژگی‌های ذاتی جعلی مقاوم باشد.

ج) شمار تلاش‌های ناموفق متوالی نباید بیش از پنج بار شود. به‌محض رسیدن به حدود مزبور، باید اقدامات ذیل انجام پذیرد:

[9] Biometric Reader
[10] Password Hint

- ایجاد وقفه زمانی حداقل سی ثانیه‌ای پیش از تلاش بعدی و افزایش زمان وقفه‌های بعدی به‌صورت نمایی (برای نمونه: یک دقیقه وقفه پس از تلاش ناموفق اول، دو دقیقه وقفه پس از تلاش ناموفق دوم و به همین ترتیب . . .) یا
- توقف فرآیند دریافت عامل ویژگی ذاتی از دارنده افزاره ارائه‌دهنده رمز پویا و پیشنهاد عاملی دیگر جهت احراز هویت (برای نمونه: شرط زیست‌سنجی متفاوت یا گذرواژه دیگر، درصورتی‌که چنین روش جایگزینی از قبل تعریف شده باشد.)

ماده ۴۰) مؤسسه اعتباری باید سازوکاری برای غیر فعال‌سازی[11] و ابطال[12] افزاره ارائه رمز پویا فراهم نماید به‌نحوی‌که قادر باشد بلافاصله پس از درخواست دارنده کارت بانکی یا در زمان وقوع رخدادهایی که دارندگان کارت را با مخاطره روبرو می‌نماید، افزاره ارائه رمز پویا را به‌صورت دائم یا موقت غیرقابل استفاده نمایند.

تبصره) مراکز شبانه‌روزی پاسخگویی به مشتریان باید از قابلیت‌های لازم برای غیرفعال سازی و ابطال افزاره‌های ارائه رمز پویا برخوردار باشند.

ماده ۴۱) مؤسسه اعتباری باید در خصوص امحاء[13] افزاره‌های ارائه رمزهای پویا فرآیندهای امنی طراحی و پیاده‌سازی کند.

ماده ۴۲) درصورتی‌که مؤسسه اعتباری، از افزاره‌های ارائه رمز پویای «قابل‌استفاده مجدد» بهره می‌برد، باید فرآیند امنی برای استفاده مجدد طراحی، پیاده‌سازی و مستندسازی کند.

ماده ۴۳) مؤسسه اعتباری باید پیش از تحویل دستگاه خاص‌منظوره ارائه رمز پویا (مانند توکن سخت‌افزاری) به دارنده کارت بانکی، از وجود کنترل‌های لازم برای جلوگیری از تغییر و دست‌کاری این دستگاه‌ها، حصول اطمینان نماید.

ماده ۴۴) مؤسسه اعتباری باید پیش از تحویل دستگاه خاص‌منظوره ارائه رمز پویا (مانند توکن سخت‌افزاری) به دارنده کارت بانکی، از وجود کنترل‌های لازم برای پیشگیری از نسخه‌برداری[14] از این دستگاه‌ها، حصول اطمینان نماید.

ماده ۴۵) درصورتی‌که مؤسسه اعتباری از مؤلفه‌های نرم‌افزاری طراحی‌شده برای دستگاه‌های چندمنظوره به‌عنوان افزاره ارائه رمزهای پویا استفاده می‌کند بایستی موارد ذیل را رعایت کند:

الف) باید از نصب نرم‌افزار روی دستگاه‌های Root یا Jail Break شده جلوگیری کند.

ب) اقدامات امنیتی لازم به‌منظور جلوگیری از مهندسی معکوس کدهای نرم‌افزار را اتخاذ نماید.

ج) اقدامات لازم در خصوص استفاده از محیط‌های اجرایی امن و مجزا[15] درون دستگاه چندمنظوره اتخاذ نماید.

راهنما: نگهداری از اطلاعات و انجام عملیات حساس ازجمله نگهداری و استفاده از کلید محرمانه تولید رمز پویا و سایر کلیدهای رمزنگاری می‌توانند با استفاده از محیط‌های اجرایی امن و مجزا درون دستگاه‌های چندمنظوره انجام پذیرند.

د) سازوکارهای لازم به‌منظور حصول اطمینان از اصالت افزاره نرم‌افزاری نصب‌شده روی دستگاه چندمنظورهٔ متعلق به دارنده کارت بانکی را به‌کارگیرد.

راهنما: برای اطمینان از اصالت افزاره نرم‌افزاری می‌توان از گواهینامه الکترونیکی معتبر استفاده کرد.

---

[11] Deactivation
[12] Revocation
[13] Destruction
[14] Replication
[15] Separated Secure Execution Environments

هـ) مؤلفه نرم‌افزاری باید به ویژگی یکتایی[۱۶] از دستگاه چندمنظوره نگاشت شود.

و) استفاده هم‌زمان از یک کلید محرمانه تولید رمز پویا یا کلیدهای رمزنگاری مورداستفاده برای انتقال امن رمزهای پویا در چند نرم‌افزار نصب‌شده مجاز نیست.

ماده ۴۶) مؤسسه اعتباری باید دارندگان کارت بانکی را از چگونگی محافظت از افزاره ارائه رمزهای پویا در برابر سرقت و اقداماتی که دارنده کارت در صورت سرقت افزاره می‌بایست به انجام رساند، آگاه سازد.

مبحث دهم- الزامات کارگزاری رمزهای پویا

ماده ۴۷) کلیدهای محرمانه مورداستفاده مؤسسه اعتباری –در سمت کارگزار– برای بازتولید رمزهای پویا، باید در مقابل سرقت، تخریب، دست‌کاری و افشای آنها نزد طرف‌های غیرمجاز محافظت شوند.

ماده ۴۸) در صورت در معرض خطر قرار گرفتن خدمت رمزهای پویا، مؤسسه اعتباری باید تهدیدات و رخدادهای شناسایی‌شده را مطابق با «الزامات گزارش‌دهی رخدادهای امنیت اطلاعات بانکی» (BIS RG 200-10) گزارش نماید.

ماده ۴۹) با توجه به اینکه مخاطرات مرتبط با خدمت رمزهای پویا در طول زمان قابل‌تغییر هستند لذا مؤسسه اعتباری باید سطح قابل‌پذیرش مخاطره را برای خدمت رمزهای پویای ارائه‌شده توسط آن مؤسسه تعیین کرده و ضمن پایش مخاطرات مرتبط با این خدمت، راهکارهای لازم را برای مقابله با مخاطرات غیرقابل‌پذیرش اتخاذ نماید.

ماده ۵۰) هرگاه بانک مرکزی مخاطره استفاده از خدمت یا افزاره‌های ارائه رمز پویا –متعلق به آن مؤسسه– را غیرقابل‌پذیرش تشخیص داد، مؤسسه اعتباری باید استفاده از آنها را متوقف نماید.

ماده ۵۱) در صورت بروز هرگونه رخداد امنیتی در محدوده خدمت رمزهای پویا که دارندگان کارت‌های صادرشده توسط مؤسسه اعتباری را در معرض خطر قرار دهد، مؤسسه باید بلافاصله دارندگان کارت‌های بانکی تحت تأثیر قرار گرفته را آگاه نموده و اقدامات واکنشی لازم به‌منظور محدود نمودن اثرات ناشی از رخدادهای مورداشاره را به انجام رساند.

ماده ۵۲) مؤسسه اعتباری باید پس از دریافت رمز پویای تکراری، در خصوص احتمال اینکه فردی به‌جز دارنده کارت (مهاجم) از آن رمز پویا استفاده کرده است، به او هشدار دهد.

ماده ۵۳) مؤسسه اعتباری باید در خصوص امحاء[۱۷] افزاره‌های ارائه رمزهای پویا، با رعایت الزامات قانونی و مقرراتی مرتبط با نگهداری اطلاعات تراکنش‌ها، دیگر اطلاعات مرتبط با افزاره‌های امحاءشده را به روشی امن از بین ببرد.

ماده ۵۴) مؤسسه اعتباری باید اطمینان یابد که اقدامات لازم در خصوص مقاوم نمودن اجزاء فناورانه، فرآیندها و رویه‌های اجرایی مرتبط با خدمت رمزهای پویا انجام‌شده است.

ماده ۵۵) مؤسسه اعتباری باید پیش از عملیاتی شدن خدمت رمزهای پویا و پس از اعمال هر تغییر قابل‌توجهی، نسبت به ارزیابی امنیتی زیرساخت‌های فناورانه، فرآیندها و رویه‌های اجرایی مرتبط با خدمت مورداشاره اقدام نموده، نتایج آن را مستند کرده و در مدیریت مخاطرات مرتبط با این خدمت استفاده نماید.

تبصره) پیش از عملیاتی شدن خدمت رمز پویا، باید مخاطرات باقی‌مانده، مستند شده و توسط مدیریت ارشد مؤسسه اعتباری به طور رسمی پذیرفته شود.

---

[۱۶] ویژگی یکتای دستگاه مانند IMEI یا سیم‌کارت در تلفن‌های همراه

[17] Destruction

ماده ۵۶) مؤسسه اعتباری باید حداقل به‌طور سالانه، اجزاء فناورانه، فرآیندها و رویه‌های اجرایی مرتبط با خدمت رمزهای پویا را مورد ارزیابی امنیتی قرار دهد. این ارزیابی باید توسط ممیزان خارجی مستقل و واجد صلاحیت‌های لازم انجام پذیرفته و از نتایج آن در مدیریت مخاطرات مرتبط با خدمت مورداشاره استفاده شود.

ماده ۵۷) گزارش ارزیابی‌های امنیتی انجام‌شده در محدوده خدمت رمز پویا باید بنا به درخواست، در اختیار بانک مرکزی ج.ا.ا قرار گیرد.

مبحث یازدهم- اقدامات انضباطی

ماده ۵۸) در صورت اعلام مراجع قضایی مبنی بر تحمیل خسارت مالی به دارندگان کارت‌های بانکی به دلیل عدم رعایت الزامات مندرج در این سند، مسئولیت جبران خسارت مورداشاره بر عهده مؤسسه اعتباری است.