



بانک مرکزی جمهوری اسلامی ایران

اداره نظام های پرداخت

الزامات امنیتی فضای تولید و تبادل اطلاعات بانکی

الزامات رمزهای پویا در تراکنش های 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 عهده 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 تأسیس شده 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 مورد استفاده قرار گیرد.



۸. اجرا

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

پیاده سازی الزامات «رمزهای پویا در تراکنش های مبتنی بر کارت» نافی مسئولیت ها و پاسخگویی بانک ها و مؤسسات اعتباری در خصوص مدیریت مخاطرات خدمات مبتنی بر کارت های بانکی نیست.

۹. زمان بندی اجرا و نظارت

الزامات «رمزهای پویا در تراکنش های مبتنی بر کارت» از تاریخ ابلاغ بانک مرکزی ج.ا.ا قابلیت پیاده سازی و اجرایی شدن توسط بانک ها و مؤسسات اعتباری را دارد.

۱۰. قوانین، مقررات و اسناد مرتبط

- «الزامات بهره برداری امن از دستگاه های 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 تراکنش های مبتنی بر کارت» از طریق پورتال اطلاع رسانی اداره نظام های پرداخت بانک مرکزی ج.ا.ا در دسترس است.

۱۲. تصویب و ابلاغ

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



فهرست مطالب

۲	بخش یکم- کلیات
۲	مبحث یکم- تعاریف
۳	مبحث دوم- هدف
۳	مبحث سوم- محدوده
۳	بخش دوم- الزامات خدمت رمزهای پویا
۳	مبحث چهارم- الزامات عمومی
۴	مبحث پنجم- مشخصات رمز پویا
۴	مبحث ششم- ثبت نام برای استفاده از خدمت رمزهای پویا
۵	مبحث هفتم- تولید رمز پویا
۵	مبحث هشتم- انتقال اطلاعات حساس
۵	مبحث نهم- الزامات افزاره های ارائه رمز پویا
۸	مبحث دهم- الزامات کارگزاری رمزهای پویا
۸	مبحث یازدهم- اقدامات انضباطی



بخش یکم- کلیات

مبحث یکم- تعاریف

ماده (۱) تعاریف و قراردادهای به کاررفته در سند حاضر به شرح ذیل اند:

(الف) مؤسسه اعتباری: بانک یا مؤسسه اعتباری غیر بانکی است که به موجب قانون یا با مجوز بانک مرکزی تأسیس شده و تحت نظارت بانک مرکزی است.

(ب) رمز اول کارت: رمز مورد استفاده توسط دارنده کارت بانکی به منظور بهره گیری از خدمات با حضور فیزیکی کارت مانند خرید با استفاده از پایانه های فروش و دریافت وجه با استفاده از دستگاه های خودپرداز.

(ج) رمز دوم کارت: رمز مورد استفاده توسط دارنده کارت بانکی به منظور بهره گیری از خدمات بدون نیاز به حضور فیزیکی کارت مانند خرید اینترنتی با استفاده از درگاه های 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 یک بار صورت پذیرد.

(ه) مهندسی اجتماعی: تلاش برای فریب افراد و ترغیب آنها به افشای اطلاعات حساس نظیر گذرواژه ها یا ترغیب آنها به انجام یک عمل خاص مانند انتقال وجه به حساب کلاهبرداران، با استفاده از ابزارهای رایانه ای یا غیر رایانه ای.

(و) احراز هویت: رویه ای است که از طریق آن مؤسسه اعتباری، هویت دارنده کارت بانکی را تصدیق کرده یا استفاده از ابزار پرداخت مشخصی را اعتباربخشی می کند.

(ز) عناصر احراز هویت: عناصری در دسته های دانستنی^۱ (آنچه تنها کاربر می داند) مانند رمز، دانستنی^۲ (آنچه تنها کاربر دارد) مانند توکن سخت افزاری و ویژگی ذاتی^۳ (آنچه کاربر هست) مانند اثر انگشت.

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

(ط) افزاره ارائه رمزهای پویا: هرگونه ابزاری اعم از مؤلفه های نرم افزاری طراحی شده برای دستگاه های چندمنظوره^۴ یا دستگاه های خاص منظوره مانند توکن های سخت افزاری که مؤسسه اعتباری به منظور ارائه رمزهای پویا در اختیار دارنده کارت بانکی قرار می دهد. در فرآیند احراز هویت دارندگان کارت در خدمات مبتنی بر کارت، افزاره ارائه دهنده رمز پویا آن چیزی است که دارنده کارت در اختیار دارد (دانستنی).

(ی) نانس: مقداری است که در الگوریتم های تولید رمز پویا، برای محاسبه رمز پویا از آن استفاده می شود. 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 ارائه دهنده رمز پویای مشخصی به صورت مادام العمر ثابت بوده و پس از ترکیب با نانس در یک الگوریتم امن منجر به تولید رمز پویا می شود.

(ل) کانال از راه دور: کانالی است برای تعامل دارنده کارت بانکی و مؤسسه اعتباری به نحوی که 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 مورد استفاده برای ارتباطات از راه دور، انجام می شود.

¹ Knowledge

² Possession

³ Inherence

^۴ 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^۶)، هویت پذیرنده ارتباط (کارگزار^۷) 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^۸ 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 MD5, DES, SHA1) 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.

^۶ Client

^۷ Server

^۸ Man-in-the-Middle



راهنما: مؤسسه اعتباری می تواند به صورت مستمر و با انتخاب روش های اثربخش، دارندگان کارت بانکی را از نحوه حفاظت از رمزهای پویا آگاه نموده و آنها را نسبت به شگردهای مورد استفاده کلاه برداران 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 مدت زمان معین، ارائه خدمت مرتبط را به دارنده کارت، به طور موقت یا دائم مسدود کند.

تبصره ۱) زمانی که مسدودسازی موقتی باشد، مدت زمان مسدودی و تعداد دفعات مسدودی را باید بر اساس ویژگی های خدمت ارائه شده 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 رویه ای 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 پیاده سازی الزامات مندرج در این سند را به طور 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 تولید شده منقضی و غیرقابل استفاده شود.

ماده ۱۵) رمزهای پویا در طول عمر خود، باید تنها یک بار 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 کارت های صادر شده توسط مؤسسه اعتباری - قابل استفاده باشند.

مبحث ششم - ثبت نام برای استفاده از خدمات رمزهای پویا

ماده ۱۷) استفاده از خدمات رمزهای پویا و جایگزینی آنها به جای رمزهای ایستا در خدمات مبتنی بر کارت، نیازمند ثبت نام دارندگان کارت بانکی است.

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

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

تبصره) ثبت نام از طریق دستگاه های خودپرداز تنها روی دستگاه هایی مجاز است که متعلق به مؤسسه اعتباری صادرکننده کارت بوده و منطبق با «الزامات بهره برداری امن از دستگاه های خودپرداز» (BIS RG 300-10) باشند.

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



ماده ۲۱) مؤسسه اعتباری تنها زمانی می تواند از شماره تلفن همراه به عنوان 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 خدمات 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 فعال سازی مجدد خدمات 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 ثبت نام مجدد (مطابق مفاد مندرج در مبحث ششم) باشد.

مبحث هفتم - تولید رمز پویا

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

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

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

ماده ۲۷) طول نانس مورد استفاده برای تولید رمز پویا باید به اندازه ای 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 هیچ یک از رمزهای پویای پیش تر تولید شده، وجود داشته باشد.

ماده ۲۹) با افشای یک رمز پویا، نباید هیچ گونه اطلاعاتی از عوامل احراز هویت، قابل استخراج باشد.

مبحث هشتم - انتقال اطلاعات حساس

ماده ۳۰) توزیع کلیدهای محرمانه مورد استفاده برای تولید رمزهای پویا باید از طریق کانال محافظت شده انجام پذیرد.

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

مبحث نهم - الزامات افزارهای ارائه رمز پویا

ماده ۳۲) مؤسسه اعتباری می تواند از افزارهای نرم افزاری یا دستگاه های خاص منظوره مانند توکن های سخت افزاری برای ارائه رمزهای پویا به دارندگان کارت بانکی استفاده کند.

ماده ۳۳) مؤسسه اعتباری باید اطمینان یابد که افزارهای ارائه رمز پویا به شیوه ای امن به دارنده کارت بانکی ارتباط داده شده است.

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

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

ماده ۳۵) استفاده هم زمان از چند افزار ارائه رمزهای پویا برای یک کارت بانکی غیر مجاز است.



ماده ۳۶) افزاره ارائه رمز پویا - به ویژه افزاره های مبتنی بر نرم افزار - باید از استخراج و کپی شدن کلید محرمانه تولید رمزهای پویا و استفاده از آنها در افزاره های 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 می داند)، یا ویژگی ذاتی (مانند مشخصه زیست سنجی از دارنده کارت) باشد.

راهنما: عوامل احراز هویت دانستنی یا ویژگی ذاتی، ممکن است از طریق یک صفحه کلید یا یک خوانشگر زیست سنجی^۹ که با افزاره ارائه دهنده رمز پویا یکپارچه شده، دریافت شود.

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

- الف)** حداقل طول عامل دانستنی در افزاره های خاص منظوره سخت افزاری معادل چهار رقم باشد.
- ب)** حداقل طول عامل دانستنی در افزاره های نرم افزاری معادل هشت کاراکتر باشد.
- ج)** در افزاره های نرم افزاری نباید از قابلیت «یادآور گذرواژه»^{۱۰} استفاده کرد.
- د)** در افزاره های نرم افزاری نباید از قابلیت «پرسش های امنیتی» استفاده کرد.
- هـ)** هنگام انتخاب یا تغییر رمز در افزاره های نرم افزاری، از انتخاب رمزهای رایج یا پرمخاطره جلوگیری گردد.
- و)** شمار تلاش های ناموفق متوالی نباید بیش از پنج بار شود. به محض رسیدن به حدود مزبور، باید اقدامات ذیل انجام پذیرد:

- ایجاد وقفه زمانی حداقل سی ثانیه ای پیش از تلاش بعدی و افزایش زمان وقفه های بعدی به صورت 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 ارائه دهنده رمز پویا و پیشنهاد عاملی دیگر جهت احراز هویت (برای نمونه: شرط زیست سنجی یا گذرواژه دیگر، در صورتی که 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 وارد کردن عامل دانستنی، کاراکترهای ورودی به صورت 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) در صورتی که عامل احراز هویت به کار گرفته شده برای استفاده از افزاره ارائه دهنده رمز پویا از نوع «ویژگی ذاتی» باشد، باید حداقل الزامات زیر برآورده شوند:

- الف)** ویژگی ذاتی از طریق یک حس گر فیزیکی دریافت شود.
- ب)** سازوکار زیست سنجی تا حد امکان در برابر ویژگی های ذاتی جعلی مقاوم باشد.
- ج)** شمار تلاش های ناموفق متوالی نباید بیش از پنج بار شود. به محض رسیدن به حدود مزبور، باید اقدامات ذیل انجام پذیرد:

^۹ Biometric Reader

^{۱۰} Password Hint



- ایجاد وقفه زمانی حداقل سی ثانیه ای پیش از تلاش بعدی و افزایش زمان وقفه های بعدی به صورت 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 ارائه دهنده رمز پویا و پیشنهاد عاملی دیگر جهت احراز هویت (برای نمونه: شرط زیست سنجی متفاوت یا گذرواژه دیگر، در صورتی که چنین روش جایگزینی از قبل تعریف شده باشد).

ماده ۴۰) مؤسسه اعتباری باید سازوکاری برای غیر فعال سازی^{۱۱} و ابطال^{۱۲} افزاره ارائه رمز پویا فراهم نماید به نحوی که قادر باشد بلافاصله پس از درخواست دارنده کارت بانکی یا در زمان وقوع رخدادهایی که دارندگان کارت را با مخاطره روبرو می نماید، افزاره ارائه رمز پویا را به صورت دائم یا موقت غیر قابل استفاده نمایند.

تبصره) مراکز شبانه روزی پاسخگویی به مشتریان باید از قابلیت های لازم برای غیر فعال سازی و ابطال افزاره های ارائه رمز پویا برخوردار باشند.

ماده ۴۱) مؤسسه اعتباری باید در خصوص امحاء^{۱۳} افزاره های ارائه رمزهای پویا فرآیندهای امنی طراحی و پیاده سازی کند.

ماده ۴۲) در صورتی که مؤسسه اعتباری، از افزاره های ارائه رمز پویای «قابل استفاده مجدد» بهره می برد، باید فرآیند امنی برای استفاده مجدد طراحی، پیاده سازی و مستندسازی کند.

ماده ۴۳) مؤسسه اعتباری باید پیش از تحویل دستگاه خاص منظوره ارائه رمز پویا (مانند توکن سخت افزاری) به دارنده کارت بانکی، از وجود کنترل های لازم برای جلوگیری از تغییر و دست کاری این دستگاه ها، حصول اطمینان نماید.

ماده ۴۴) مؤسسه اعتباری باید پیش از تحویل دستگاه خاص منظوره ارائه رمز پویا (مانند توکن سخت افزاری) به دارنده کارت بانکی، از وجود کنترل های لازم برای پیشگیری از نسخه برداری^{۱۴} از این دستگاه ها، حصول اطمینان نماید.

ماده ۴۵) در صورتی که مؤسسه اعتباری از مؤلفه های نرم افزاری طراحی شده برای دستگاه های چند منظوره به عنوان افزاره ارائه رمزهای پویا استفاده می کند بایستی موارد ذیل را رعایت کند:

الف) باید از نصب نرم افزار روی دستگاه های Root یا Jail Break شده جلوگیری کند.

ب) اقدامات امنیتی لازم به منظور جلوگیری از مهندسی معکوس کدهای نرم افزار را اتخاذ نماید.

ج) اقدامات لازم در خصوص استفاده از محیط های اجرایی امن و مجزا^{۱۵} درون دستگاه چند منظوره اتخاذ نماید.

راهنما: نگهداری از اطلاعات و انجام عملیات حساس از جمله نگهداری و استفاده از کلید محرمانه تولید رمز پویا و سایر کلیدهای رمزنگاری می توانند با استفاده از محیط های اجرایی امن و مجزا درون دستگاه های چند منظوره انجام پذیرند.

د) سازوکارهای لازم به منظور حصول اطمینان از اصالت افزاره نرم افزاری نصب شده روی دستگاه چند منظوره متعلق به دارنده کارت بانکی را به کارگیرد.

راهنما: برای اطمینان از اصالت افزاره نرم افزاری می توان از گواهی نامه الکترونیکی معتبر استفاده کرد.

¹¹ Deactivation

¹² Revocation

¹³ Destruction

¹⁴ Replication

¹⁵ Separated Secure Execution Environments



ه) مؤلفه نرم افزاری باید به ویژگی یکتایی^{۱۶} از دستگاه چندمنظوره نگاشت شود.

و) استفاده هم زمان از یک کلید محرمانه تولید رمز پویا یا کلیدهای رمزنگاری مورد استفاده برای انتقال امن رمزهای پویا در چند نرم افزار نصب شده 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 می بایست به انجام رساند، آگاه سازد.

مبحث دهم- الزامات کارگزاری رمزهای پویا

ماده ۴۷) کلیدهای محرمانه مورد استفاده مؤسسه اعتباری -در سمت کارگزار- برای بازتولید رمزهای پویا، باید در مقابل سرقت، تخریب، دست کاری و افشای آنها نزد طرف های غیرمجاز محافظت شوند.

ماده ۴۸) در صورت در معرض خطر قرار گرفتن خدمت رمزهای پویا، مؤسسه اعتباری باید تهدیدات و رخدادهای شناسایی شده را مطابق با «الزامات گزارش دهی 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 قابل تغییر هستند لذا مؤسسه اعتباری باید سطح قابل پذیرش مخاطره را برای خدمت رمزهای پویای ارائه شده توسط آن مؤسسه تعیین کرده و ضمن پایش مخاطرات مرتبط با این خدمت، راهکارهای لازم را برای مقابله با مخاطرات غیرقابل پذیرش اتخاذ نماید.

ماده ۵۰) هرگاه بانک مرکزی مخاطره استفاده از خدمت یا افزاره های ارائه رمز پویا -متعلق به آن مؤسسه- را غیرقابل پذیرش 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 کارت های صادر شده توسط مؤسسه اعتباری را در معرض خطر قرار دهد، مؤسسه باید بلافاصله دارندگان کارت های بانکی تحت تأثیر قرار گرفته را آگاه نموده و اقدامات واکنشی لازم به منظور محدود نمودن اثرات ناشی از رخدادهای مورد اشاره را به انجام رساند.

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

ماده ۵۳) مؤسسه اعتباری باید در خصوص امحاء^{۱۷} افزاره های ارائه رمزهای پویا، با رعایت الزامات قانونی و مقرراتی مرتبط با نگهداری اطلاعات تراکنش ها، دیگر اطلاعات مرتبط با افزاره های امحاء شده 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 رویه های اجرایی مرتبط با خدمت رمزهای پویا انجام شده است.

ماده ۵۵) مؤسسه اعتباری باید پیش از عملیاتی شدن خدمت رمزهای پویا و پس از اعمال هر تغییر قابل توجهی، نسبت به ارزیابی امنیتی زیرساخت های فناورانه، فرآیندها و رویه های اجرایی مرتبط با خدمت مورد اشاره 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 باقی مانده، مستند شده و توسط مدیریت ارشد مؤسسه اعتباری به طور رسمی پذیرفته شود.

^{۱۶} ویژگی یکتای دستگاه مانند IMEI یا سیم کارت در تلفن های همراه

^{۱۷} 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 مورد اشاره 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 مورد اشاره بر عهده مؤسسه اعتباری است.