بسمه تعالی

بانک مرکزی جمهوری اسلامی ایران

اداره نظام‌های پرداخت

چارچوب راهبرد راهبری و مدیریت کارت هوشمند در شبکه بانکی کشور

۱۳۸۴/۱/۱۵

الف. کلیات

اشکالات مندرج در فنآوری کارت بانک‌های مغناطیسی که بیش از چهار دهه از عمر آن می‌گذرد از دو جنبه مهم نقائص ایمنی و محدودیت‌های فنی در انجام تراکنش صنعت بانکداری را بر آن داشته تا استفاده از تراشه‌کارت‌ها[1] را به عنوان جایگزین مناسب مد نظر قرار دهد. تراشه‌کارت‌های دارای پردازنده و حافظه که قابلیت اجرای برنامه‌های کاربردی را در پایانه‌های مربوط داشته باشند، تحت نام کارت‌های هوشمند طبقه‌بندی گردیده‌اند. کارت‌های هوشمند به بانک‌ها امکان می‌دهند تا اولاً ایمنی انجام تراکنش‌ها را، که در سال‌های اخیر در کاربری کارت‌های مغناطیسی به شدت کاهش یافته‌اند، تا حد قابل قبولی تضمین کنند و ثانیاً با نصب برنامه‌های کاربردی مختلف درون تراشه روی کارت امکانات جدیدی به کارت‌بانک بیافزایند که از جمله می‌توان به امکان کاربری برونخط[2] کارت‌بانک اشاره نمود. در سال‌های اخیر با کاهش قابل توجه بهای این گونه کارت‌ها و همچنین افزایش هزینه‌های ناشی از سوءاستفاده و کلاهبرداری از کارت‌های مغناطیسی، گرایش به جایگزینی کامل فنآوری قدیمی با فنآوری هوشمند در سطح بین‌المللی ایجاد شده و مقرر گردیده صدور کارت‌های مغناطیسی از پایان سال ۲۰۰۵ میلادی در بانک‌های عضو شبکه‌های جهانی پرداخت[3] متوقف گردد و کاربری کارت‌ها مزبور نیز به تدریج و با انقضای اعتبار کارت‌های موجود پایان یابد.

---

[1] Chip-Cards

[2] Off-Line

[3] نظیر Visa و Master Card

بانک مرکزی جمهوری اسلامی ایران نیز با همکاری شبکه بانکی و با در نظر داشتن الزامات مربوط به شبکه بانکی در در جنبه ارایه خدمات نوین به مشتریان و تطابق کامل با استانداردها و رویه‌های بین‌المللی، با انجام کارشناسی فشرده طی نیمه دوم سال ۱۳۸۲ و سه ماهه اول ۱۳۸۳ راهبرد شبکه بانکی در خصوص صدور، کاربری و راهبری کارت‌بانک‌های هوشمند را در دو فاز استانداردهای عمومی (۱۳۸۳/۴/۲۵) و مشخصات برنامه کاربردی (۱۳۸۳/۷/۱۴) ابلاغ نموده و تمهیدات مربوط به مدیریت ایمنی و زیرساخت کلید عمومی[4] را نیز در در رو بخش اخذ شناسه مرجع (۱۳۸۳/۸/۱) از مرجع بین‌المللی و راه‌اندازی مرکز گواهی (۱۳۸۳/۸/۲۵) صورت داده است. در این راستا کارت‌های هوشمند استاندارد نیز با اخذ گواهی از بانک مرکزی جمهوری اسلامی ایران در تاریخ ۱۳۸۳/۱۰/۱۲ برای اولین بار توسط بانک ملت صادر گردیده و در اختیار مشتریان قرار می‌گیرد.

با توجه به این که مدیریت و راهبری کارت‌های هوشمند چه به لحاظ سازمانی و چه به لحاظ فنی دارای پیچیدگی‌های به مراتب بیشتری است، بانک مرکزی همسو با فراهم‌آورندگان فنآوری‌های مزبور، استانداردهای مدیریت و راهبری را در دو لایهٔ استانداردهای کلی و مشخصات کاربردی تعیین نموده و الزامات مربوط به آنها را نیز فراهم ساخته است. صدور، کاربری و راهبری کارت‌بانک‌های هوشمند به علت اهمیت فراوان امکان پردازش برونخطی تراکنش‌ها در بستر مخابراتی بالنسبه ضعیف کشور از یکسو و تطابق با الزامات بین‌المللی از سوی دیگر برای شبکه بانکی حائز اهمیت فراوان بوده و بدین منظور در اولویت‌های اول بانک مرکزی جمهوری اسلامی ایران در سال ۱۳۸۳ قرار داشته است.

ب. استانداردهای صدور و پذیرش کارت‌بانک‌های هوشمند

مشخصات EMV 4.0 (2000) به عنوان استاندارد صدور کارت‌بانک‌های هوشمند، پایانه‌های قابل استفاده و تجهیزات سخت‌افزاری و نرم‌افزارها در شبکه بانکی کشور تعیین گردیده است. این مشخصات توسط اتفاق سه مرجع بین‌المللی راهبری شبکه‌های پرداخت کارتی[5] که مجموعاً بیش از ۹۰ درصد کل کارت‌بانک‌های صادر شده جهان را پوشش می‌دهند و بر اساس استانداردهای بین‌المللی زیر تدوین شده است:

۱. ISO/IEC 7811-1: 1995 (روش‌های برجسته‌نگاری روی کارت)
۲. ISO/IEC 7811-3: 1995 (جایگذاری برجسته‌نگاری روی کارت)
۳. ISO/IEC 7816-1: 1998 (مشخصات فیزیکی کارت هوشمند)
۴. ISO/IEC 7816-2: 1999 (ابعاد و مشخصات اتصال تراشه)
۵. ISO/IEC 7816-3: 1997 (پروتکل سیگنال و انتقال آن)

[4] Public Key Infrastructure (PKI)
[5] Europay, MasterCard, Visa (EMV)

۶. ISO/IEC 7816-4: 1995 (فرمان‌های کارت هوشمند)

۷. ISO/IEC 7816-5: 1994 (شماره‌گذاری و ثبت دامنه کارت‌های هوشمند)

۸. ISO/IEC 10373: 1993 (روش‌های آزمون)

با توجه به تایید این مشخصات توسط مراجع بین‌المللی بانکی و همچنین جامعیت این استاندارد در زمینه صدور و پذیرش کارت‌بانک‌های هوشمند، کارشناسی امر به این نتیجه رسید که مشخصات فوق به عنوان استاندارد داخلی شبکه بانکی کشور – بدون جرح و تعدیل در آن – اعلام گردد. بر این اساس مشخصات مزبور در تاریخ ۱۳۸۳/۴/۲۵توسط بانک مرکزی جمهوری اسلامی ایران به عنوان استاندارد شبکه بانکی ابلاغ گردید. همچنین با توجه به اهمیت موضوع، تعیین و ارتقای استانداردها و مشخصات فنی سوئیچ شتاب بمنظور پشتیبانی از تراکنش‌های کارت‌بانک‌های هوشمند و تراکنش‌های برونخطی در دستور کار قرار گرفته و این مرکز از ابتدای آذر ۱۳۸۳ به صورت برخط و از سه ماهه اول ۱۳۸۴ به صورت برونخط تراکنش‌های مربوط به کارت‌بانک‌های هوشمند را بر اساس استاندارد اعلام شده پشتیبانی می‌کند.

همچنین در خصوص استاندارد مربوط به کیف پول الکترونیک، با توجه به اجماع بین‌المللی مشخصات کیف پول الکترونیک عمومی[6] نسخه ۱۹۹۹ به عنوان استاندارد صدور و پذیرش معین گردید.

پ. مشخصات کاربردهای کارت‌بانک‌های هوشمند

با توجه به لزوم ارایه خدمات کارت‌بانک‌های هوشمند به صورت یکسان در سطح شبکه بانکی و ارایه شناسه برنامه کاربردی[7] (مطابق با مشخصات EMV 4) به بانک‌های عضو مرکز «شتاب»، معرفی خدمات پایه کارت بانک هوشمند با توجه به استانداردهای مورد قبول بین‌المللی مد نظر بانک مرکزی جمهوری اسلامی ایران قرار گرفته است. در این خصوص مشخصات مؤسسه بین‌المللی ویزا در خصوص کارت‌های اعتباری و کارت‌های برداشت هوشمند[8] نسخه 1.4.0 و با عنایت به تطابق بیش از دو سوم کلیه کارت بانک‌های هوشمند جهان از مشخصات مزبور، به عنوان مبنای کار تعیین گردیده و با توجه به الزامات بومی سازی و لحاظ موارد ضروری در مشخصات مذکور از کلیه بانک‌ها در این خصوص نظرسنجی به عمل آمد. در نهایت با توجه به موافقت کلیه بانک‌ها در پذیرش استاندارد مذکور در سطح رابط[9]های عمده، مشخصات مزبور بدون تغییر یا اصلاح به عنوان استاندارد شبکه بانکی در زمینه کاربری کارت‌بانک‌های هوشمند اعلام گردید. این مشخصات سه ویژگی عمدهٔ کارت‌های بانکی را در بر می‌گیرد:

---

[6] Common Electronic Purse Specifications (CEPS)
[7] Application Identifier (AID)
[8] Visa Smart Debit Credit (VSDC), VIS 4.1.0
[9] Interface

۱. کارت برداشت[۱۰]
۲. کارت اعتباری[۱۱]
۳. کیف پول الکترونیک[۱۲] رمزدار

همچنین در این راستا اخذ شناسه ثبت شده[۱۳] توسط بانک مرکزی از مراجع ذیربط[۱۴] بمنظور ثبت و تولید شناسه کاربرد شبکه بانکی در دستور کار قرار گرفته و نهایتاً شناسه رسمی نظام پرداخت بانک مرکزی جمهوری اسلامی ایران با شماره A000000288 در تاریخ اول آبان ۱۳۸۳ تخصیص یافته و اعلام گردیده است.

از سوی دیگر با توجه به اهمیت کیف پول الکترونیک در انجام پرداخت‌های بسیار خُرد (پرداخت‌های مربوط به تاکسی، مترو، بنزین، خواروبار و نظایر آنها با مبلغ کمتر از ۵۰۰ هزار ریال) و همچنین اثر قابل توجه آن بر کاهش حجم تراکنش‌های کوچک بانکی و با عنایت به این که در حال حاضر اقدامات پراکنده‌ای توسط ارگان‌ها و نهادهای مختلف در این خصوص در حال انجام است؛ استاندارد سازی استفاده از کیف پول الکترونیک بدون‌رمز را در سطح ملی مورد توجه قرار داده و با توجه به لزوم کنترل حجم پول الکترونیک و لزوم انتشار آن توسط شبکه بانکی، مشخصات فنی مؤسسه بین‌المللی ویزا را در خصوص کیف پول الکترونیکی بدون رمز[۱۵] به عنوان مبنای کار مد نظر قرار داده و نهایتاً با توجه به موافقت کلیه اعضای شبکه بانکی مشخصات مزبور به عنوان استاندارد کاربری کارت‌بانک هوشمند به عنوان کیف پول الکترونیک بدون رمز به شبکه بانکی کشور ابلاغ گردید.

ت. ملاحظات حفاظتی و امنیتی

استفاده از فنآوری کارت‌بانک‌های هوشمند با وجود مزایای آشکار، پیچیدگی‌های فنی و سازمانی بسیار بیشتری نسبت به مدیریت کارت بانک‌های مغناطیسی داشته بر این اساس می‌باید تنظیمات مقرراتی و سازمانی متناظر با آن تدوین و اجرایی گردد. یکی از موارد اساسی در شیوه صدور کارت‌بانک‌های هوشمند و انجام تراکنش‌های بانکی از طریق آن در پایانه‌ها، بهره‌گیری از سه مرحله تصدیق الکترونیکی داده‌ها با استفاده از رمزنگاری نامتقارن[۱۶] است که توسط زوج کلیدهای عمومی[۱۷] و خصوصی[۱۸] صورت

---

[10] Debit Card
[11] Credit Card
[12] E-Purse
[13] Registered Identifier
[14] APACS (UK)
[15] No-PIN e-purse (Visa Cash Electronic Purse Specifications: VCEPS)
[16] Asymmetric Cryptography
[17] Public Key
[18] Secret Key

می‌پذیرد[19]. از آنجایی که ایمنی کلی شبکه پرداخت کارت‌بانک‌های هوشمند مبتنی بر محرمانگی و امنیت این کلیدهاست و از آنجایی که زوج کلید عمومی می‌باید توسط مرکزی که مورد قبول تمامی صادرکنندگان قرار داشته و سرپرستی نظام جامع پرداخت را بر عهده داشته باشد اعلام شود، بدیهی به نظر می‌رسد که تعیین و اعلام کلید عمومی کارت‌های هوشمند شبکه بانکی و همچنین تایید کلیدهای عمومی تک تک اعضای آن توسط کلید خصوصی خاص، باید توسط بانک مرکزی صورت پذیرد. این مرکز وظایف زیر را بر عهده خواهد داشت:

- مدیریت کلیدها در شرایط عادی: شامل برنامه‌ریزی، تولید، توزیع، استفاده و انقضاء.
- مدیریت کلیدها در شرایط اضطراری: شامل تشخیص، برآورد، تصمیم‌گیری و ابطال پیش از موعد.
- مدیریت انقضای کلیدها در سطح شبکه بانکی.

در این راستا بانک مرکزی جمهوری اسلامی مرکز گواهی خاص کارت‌بانک‌های هوشمند را از ابتدای آذرماه ۱۳۸۳ عملیاتی نموده و کلیدهای عمومی خود را به بانک‌های کشور اعلام نموده است و تا کنون برای بانک ملت گواهینامه کاربرد کارت برداشت و کارت اعتباری در چهارچوب مشخصات VSDC صادر نموده است.

پ. پیشنهاد

- صدور و کاربری کارت‌های هوشمند باید با توجه به استانداردهای مورد قبول بین‌المللی و همچنین کاربری‌های رایج صورت پذیرد و در این خصوص حتی‌المقدور از استفاده از فنآوری‌های ناشناخته یا بومی‌ساختن بیش از حد اجتناب گردد. این امر از دو جنبه حائز اهمیت است، اولاً راهبری و ارتقای فنآوری با توجه به رعایت استانداردها موجب کاهش هزینه‌های آتی شده و ثانیاً از وابستگی به ارایه‌دهنده فنآوری خاص با توجه به گسترهٔ وسیع عرضه‌کنندگان استاندارد اجتناب به عمل خواهد آمد. ذکر این نکته ضروری است که معمولاً کاربری کارت هوشمند بازهٔ زمانی طولانی‌تر (تا ده سال) را در بر گرفته و نوعاً بهای هر واحد آن نیز از کارت‌های مغناطیسی به مراتب بالاتر است؛ از این رو آینده‌نگری در این خصوص با توجه به تحولات سریع فنآوری ضرورت خواهد داشت.
- به طور خاص، شبکه بانکی شریان اقتصادی هر کشور به شمار می‌رود که تمامی مبادلات اصلی اقتصاد از طریق آن جریان می‌یابد. از این رو حفظ ایمنی این شبکه و جلوگیری از نفوذ یا

[19] در خصوص جزئیات بیشتر عملکرد این مکانیزم می‌توان به کتابچه دوم EMV (Security & Key Management) و همچنین منابع متعدد مربوط به شیوه رمزنگاری RSA رجوع کرد.

خرابکاری در آن از اولویت اول برخوردار بوده و سایر امور نظیر امکانات و ویژگی‌های اضافی در اولویت‌های بعدی قرار می‌گیرند. با توجه به این که کارت‌های هوشمند تقریباً رایانهٔ کاملی به اندازه یک کارت به شمار می‌روند، تنوع ایجاد کاربری‌های ممکن در آن بسیار زیاد است؛ مع‌الوصف با توجه به حفظ ایمنی تراکنش‌های بانکی می‌باید کماکان از جاه‌طلبی‌های فنی پرهیز گردیده و تا حد امکان از خلط کاربری‌های دیگر با کاربری بانکی کارت‌های هوشمند اجتناب به عمل آید.