به نام خدا

پدافند غیر عامل باید همچون شعله‌ای بلند شود.

مقام معظم رهبری

پدافند غیرعامل–کارت هوشمند

فهرست:

مقدمه

امروزه سیستم های مبتنی بر کارت هوشمند به طور گسترده در سراسر د نیا رایج گردیده و رشد ناگهانی اینترنت و ارتباطات، باعث تغییرات سریع در نحوه ارتباط ما با دیگران شده است. هرچه نقش و جایگاه ارتباطات در جهان گسترده تر می گردد؛ مدل های تجارتی و سرویس دهی نیز از حالت سنتی رو در رو به سمت ارتباطات برخط[۱] در حال تغییر است. سرویس دهی الکترونیک فرصت های زیادی برای خدمت رسانی بهتر به مردم ایجاد کرده است.

کارت هوشمند که یکی از ابزارهای ارائه خدمات است، یک کارت پلاستیکی در اندازه کارت اعتباری است که در آن یک یا چند تراشه مدار قرار گرفته و می تواند از یک یا چند تکنولوژی قابل تشخیص توسط ماشین نظیر بارکد، اطلاعات بیومتری، یا شناسایی تصویر استفاده کند.

به بیان ساده کارت هوشمند، کامپیوتری است که روی یک کارت پلاستیکی تعبیه شده است (از این رو کارت هوشمند یک سیستم جاسازی[۲] شده نامیده می شود). تلفیق یک کارت پلاستیکی معمولی و یک ریزپردازنده اجازه می دهد که مقدار

---

[۱] Online

[۲] Embeded

زیادی اطلاعات به صورت برخط یا برونخط[۱] در کارت هوشمند ذخیره، پردازش و قابل دسترس شود.

ابزارهای مبتنی بر کارت و کارت خوان ها به دلیل سهولت استفاده از سوی کاربران و مدیریت از سوی سازمان های مربوطه به سرعت رو به گسترش است.

کارت های هوشمند می توانند چند صدبار بیشتر از یک کارت نوار مغناطیسی (به عنوان مثال کارت های بانکی جهت برداشت پول از سامانه های خودپرداز) داده ذخیره کنند و با ذخیره الگوریتم های رمزنگاری امنیت تبادلات را بهبود بخشند.

کامپیوتر موجود بر روی کارت هوشمند، یک تراشه مدار مجتمع است که شامل: واحد پردازش، سیستم حافظه و خطوط ورودی/خروجی است.

به طور کلی به کارت هایی که بر روی آنها اتصال طلایی وجود دارد؛ کارت های تراشه گفته می شود. کارت های هوشمند یکی از انواع کارت های تراشه می باشد. یک کارت ریزپردازنده متداول و غیر اختصاصی می تواند امنیت منطقی را به همراه داشته باشد ولی این به تنهایی برای یک کارت هوشمند کافی نیست؛ مهاجمین می توانند با استفاده از تکنیک هایی که تراشه را مستقیماً مورد

---

[۱] Off line

تهاجم قرار می دهند و یا اطلاعات را از یک ابزار عملیاتی استخراج می کنند، در برابر امنیت منطقی کارت های تراشه ریزپردازنده مقاومت کنند؛ در حالی که ریزپردازنده ای که در کارت هوشمند استفاده می شود می بایست به گونه ای طراحی شود که در برابر دستکاری مقاوم باشد. بنابراین کارت هوشمند، کارتی است که تراشه ریزپردازنده آن در برابر دستکاری مقاوم بوده و در برابر حملات شناخته شده، اقدامات متقابل انجام می دهد و به همین دلیل کپی یا جعل آن سخت می باشد. این کارت می تواند در انتقالات الکترونیکی خودکار وارد شده، داده ها را به صورت امن ذخیره نماید و بعضی از پروتکل ها و الگوریتم های امن را اجرا نماید.

پردازش امن دلیل اصلی استفاده از کار ت های هوشمند است. این کارت ها کاربردهایی از قبیل کنترل دسترسی، تجارت الکترونیک، تعیین هویت و ... دارند. بواسطه اهمیت این کاربردها، رعایت ملاحظات امنیتی برای تولیدکنندگان و کاربران کارت هوشمند، حیاتی است.

این نکته بسیار حائز اهمیت است که اگر به کارگیری و پیاده سازی سامانه کارت هوشمند با تدابیر و ملاحظات پدافندغیرعامل، توام نباشد؛ باتوجه به اهمیت کاربردهای ذکر شده برای کارت از یک سو و بکارگیری سامانه کارت هوشمند به عنوان

بستر پیاده سازی این کاربردها از سوی دیگر، می تواند نقطه تهدیدی برای کشور بشمار آید.

با توجه به اهمیت مقوله امنیت در حوزه کارت های هوشمند و نیاز به شناسایی تهدیدهای مؤثر که بخش های مختلف کارت هوشمند را تحت تاثیر قرار می دهند، مبحث دفاع و پیشگیری در برابر حملات و تهدیدات مؤثر در چرخه تولید، توسعه و بکارگیری مطرح می شود. با گسترش رو به رشد این فناوری در کشور و مواجه شدن با محدودیت های فناوری دفاعی در چرخه عمر کارت، می بایست متناسب با قابلیت های موجود در کشور راهکارهای دفاعی در برابر تهدیدات، شناسایی و معرفی شوند.

در این کتابچه، ابتدا کاربردها و معماری کارت هوشمند شرح داده شده و اشاره ای به استانداردهای مطرح در این حوزه خواهد شد، در ادامه نیازها و ویژگی های امنیتی مورد نیاز در طراحی سامانه این کارت ها از منظر پدافند غیرعامل بررسی می شود.

فصل ۱ - تاریخچه

تاریخچه اقدامات انجام شده در زمینه فناوری کارت های هوشمند و رخدادهای مربوطه بشرح ذیل ارائه می گردد:

تاریخ	اقدام/رخداد	سازمان اقدام کننده
۱۹۵۰	انتشار کارت‌های پلاستیکی	Diner Club- آمریکا
۱۹۶۸	اختراع کارت تراشه	محققین: Helmut Grottrup و Jurgen Dethloff
۱۹۷۴	اولین ایده در مورد کارتهای حافظه‌دار	Ronald Moreno (فرانسوی)
۱۹۷۷	اختراع اولین کارت تراشه ریزپردازنده	Honeywell Bull
۱۹۷۹	اختراع اولین کارت هوشمند	BullHoneywell, Motorola
۱۹۸۳	استفاده عمومی از کارت‌های تراشه در تلفنهای اعتباری	فرانسه
۱۹۹۲	دومین کاربرد محتمع سازی ریزتراشه‌ها به صورت کارتهای Debit	فرانسه
دهه ۱۹۹۰	معرفی سیستم موبایل GSM مبتنی بر SIM	اروپا
۱۹۹۳	توافقات همکاری برای طراحی و بکارگیری کارت‌های هوشمند در انواع کارتهای	مستر کارت، ویزا، و Europay

تاریخ	اقدام/رخداد	سازمان اقدام کننده
	Debit و Credit	
۱۹۹۴	ظهور اولین نسخه EMV	مستر کارت، ویزا، و Europay
۲۰۰۰ و ۲۰۰۴	ارتقای EMV	EMV Co.
۲۰۰۵	طرح یک آسیا - یک کارت	کشورهای کره، چین، و سنگاپور
۲۰۰۵	طرح کارت راه ابریشم	کشورهای کره، چین، و سنگاپور
۱۳۸۴	طرح نحوه و میزان بکارگیری امنیت در فناوریهای اطلاعاتی مانند کارتهای هوشمند	شورای عالی امنیت فضای تبادل اطلاعات کشور
۱۳۸۶	طرح کارت هوشمند چند منظوره (ایران کارت	وزارت ارتباطات و فناوری اطلاعات
۱۳۸۶	کارت هوشمند سوخت	شرکت ملی پخش فراورده‌های نفتی ایران
۱۳۸۶	حکمت کارت و ثمین کارت	شرکت ایزایران
۱۳۸۶	اجرای طرح آزمایشی صدور کارت هوشمند برای بیماران خاص در سمنان	سازمان بیمه خدمات درمانی

فصل ۲ - کارت هوشمند و نقش آن در جامعه اطلاعاتی

در شرایط کنونی دولت ها بدون استفاده از فناوری اطلاعات نمی توانند برخی از فرایندهای مدیریت، تصمیم گیری و تصمیم سازی در سطح ملی را به نحو مطلوب به انجام برسانند.

سازمان های دولتی با توسعه کاربری فناوری ارتباطات و اطلاعات در فرایندها و روش های خود موفق به ارائه بهتر و سریع تر خدمات به شهروندان شده اند و با این رویکرد، کاربرد فناوری اطلاعات در مدیریت، ساماندهی و ارائه خدمات دولتی با ایده دولت الکترونیک محقق شده است.

در ایران نیز بسیاری از سازمان ها توسعه کارت هوشمند را در تکمیل فرایند خدمات رسانی الکترونیکی انتخاب نموده اند و مطالعات اولیه را برای توسعه این فناوری در سازمان های خود انجام داده اند. نظر به توسعه روزافزون کارت هوشمند و کابردهای آن در سطح بین المللی و توجه سازمان های داخل کشور به ارائه خدمات از طریق کارت های هوشمند، می بایست برنامه ریزی هایی در خصوص امن، ایمن و پایدار نمودن کارت های هوشمند مورد استفاده، پیش از گام برداشتن جهت توسعه این فناوری صورت پذیرد.

مهمترین دلیل گسترش کاربرد کارت های هوشمند در حوزه های مختلف، قابلیت آن ها در فراهم نمودن امنیت و راحتی استفاده از آن ها است. کارت های هوشمند می توانند حجم قابل توجهی از اطلاعات را پردازش، ذخیره و حمل نمایند؛ از این منظر این کارت ها در صورت عدم توجه کافی به ملاحظات پدافندغیرعامل مرتبط می توانند همچون یک شمشیر دولبه در جهت خلاف خواسته توسعه دهندگانشان حرکت کنند.

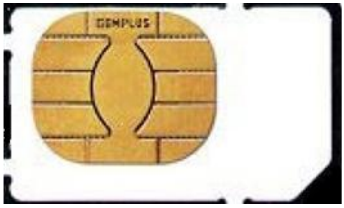
با توسعه قدرت ریز پردازنده موجود بر روی کارت و همچنین توسعه ظرفیت نگهداری اطلاعات، کاربرد کارت هوشمند به حوزه های بیشتری توسعه یافته است . یکی از کاربردهای مهم کارت های هوشمند در حوزه تراکنش های مالی است. امروزه کاربرد کارت های هوشمند به حوزه های دیگر نظیر درمان، حمل و نقل، تشخیص هویت، دسترسی و غیره نیز توسعه یافته است.

در حال حاضر برای جلوگیری از صدور کارت های هوشمند متعدد برای کابردهای مختلف، رویکرد جهان به سمت استفاده از کارت های هوشمند چند کاربردی است. بنابراین کاربردهایی که نیازهای امنیتی مشابه دارند در یک کارت گنجانده می شوند و در مقابل ضریب امنیتی کارت مجتمع حاصل تا جای ممکن تقویت می شود.

برخی از کاربردهای کارت هوشمند در زندگی امروز به قرار ذیل می باشد:

تلفن های همراه

یکی از کاربردهای کارت های هوشمند استفاده از آن ها در تلفن های همراه است . در این کاربرد، از کارت های هوشمند به صورت فیزیکی استفاده نمی شود؛ بلکه این کارت ها به عنوان یک بخش ثابت رمزکننده و تصدیق اصالت در قالب یک سیم[1] کارت مورد استفاده قرار می گیرند. در واقع تلفن های همراه از یک ماژول امنیتی که در سیم کارت جاسازی شده است؛ استفاده می نمایند.



سیستم های پرداخت الکترونیک

یکی از محاسن کارت هوشمند این است که به افراد اجازه می دهد که از آن به عنوان کیف پول الکترونیکی استفاده کنند. در حالی که کارت های اعتباری در پرداخت خود تأخیر دارند و هزینه

[1] SIM: Subscriber Identification Module

کارت های بدهی[۱] باید بلافاصله پرداخت شود[۲]، سیستم کیف پول الکترونیک، پیش پرداخت است[۳].

از دیگر کاربردهای مالی کارت های هوشمند دفترچه حساب پس انداز الکترونیکی می باشد. در دفترچه حساب های بانکی سنتی، با استفاده از رکوردهای چاپ شده در دفترچه می توان سوابق حساب بانکی را به دست آورد، اغلب این نوع دفترچه های حساب پس انداز، به دلیل ضعف های امنیتی دارای یک نوار مغناطیسی می باشند که همه یا بخشی از داده های چاپ شده در دفترچه، روی آن نیز کپی شده است. استفاده از کارت های هوشمند، اجازه می دهد دارنده حساب کاربری به صورت مطمئن تری شناسایی شود. بانک ها می توانند اطلاعات بیشتری را بر روی کارت هوشمندی که در دست مشتریان قرار دارد، نگهداری کنند و این امر، امکان فراهم کردن خدمات بیشتر را در نقاط دور افتاده ای که دسترسی برخط وجود ندارد یا ممکن است کند باشد، فراهم می نماید. کارت های هوشمند همچنین می توانند هزینه عملیات ها را کاهش داده و سیستم های درآمدی جدید تولید کنند.

---

[۱] Debit Card

[۲] Pay Now

[۳] Prepaid

بوسیله کارت های هوشمند بانکی، می توان علاوه بر گسترش امنیت، یک عاملیت جدید به شکل تراکنش های برون خط، که توسط رمزنگاری کلید عمومی پشتیبانی می شود را به خدمات ارائه شده، اضافه نمود.

شناسایی

از آنجا که هر روزه سیستم های محلی و دولتی هرچه بیشتر به سمت فرایندها و تراکنش های الکترونیکی حرکت می کنند و بمنظور ارائه خدمات بهتر، سریع تر و امن، ایمن و پایدار تر به شهروندان، داشتن نوعی هویت الکترونیکی راحت و مناسب، با اعمال ملاحظات پدافند غیر عامل در جهت بالا بردن آرامش روانی جامعه و افزایش سرعت پذیرش چنین هویتی برای شهروندان، امری اجتناب ناپذیر است.

کنترل دسترسی به کامپیوترها، مکان ها و اطلاعات

دسترسی به اکثر رایانه ها با ترکیبی از نام و گذرواژه کاربر امکانپذیر است. گذرواژه را می توان با نگاه به دست کاربر، یادداشتهای جامانده در کنار رایانه، بازبینی ترافیک داده و یا در برخی موارد هک فایل های سیستمی، بدست آورد. روش مطمئن تر

کنترل، شامل استفاده از توکنی هوشمند[۱]، مانند یک کارت هوشمند می باشد. شناسه کاربر می تواند هم توسط کارت و هم توسط کاربر فراهم شود و گذرواژه نیز توسط کارت چک می شود. ممکن است کارت دارای یک پروفایل کاربر باشد که در آن سطح دسترسی کاربر برای دستیابی به توابع سیستمی خاص ثبت شده باشد. همچنین کارت می تواند محدوده ای از گذرواژه ها و مکانیزم های هویت شناسی را در خود ذخیره کند، بنابراین کاربر یکبار خودش را به کارت می شناساند و پس از آن نیازی ندارد که تعداد زیادی گذرواژه را برای عبور از دیواره آتش، دسترسی به وب سایت ها، اجازه دریافت پول و بسیاری موارد دیگر به خاطر بسپارد.

[۱] Smart token

فصل ۳ - معماری کلان کارت های هوشمند

❖ سخت‌افزار کارت هوشمند

سخت‌افزار کارت هوشمند به دو بخش اصلی تقسیم می‌شود:

- بدنه پلاستیکی
- میکروماژول[۱]

میکروماژول جاسازی شده در کارت‌های هوشمند شامل دو بخش ریزاتصال[۲] و ریزتراشه[۳] یا همان میکروکنترلر است. میکروماژول اجازه اجرای دستورالعمل‌های پشتیبانی از کارت را به

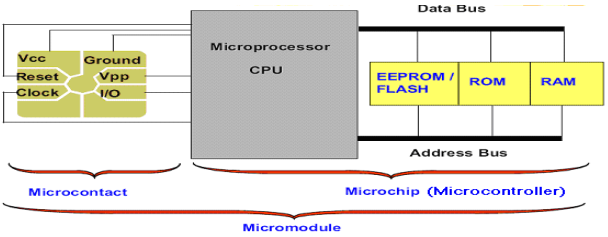
---

[۱] Micromodule

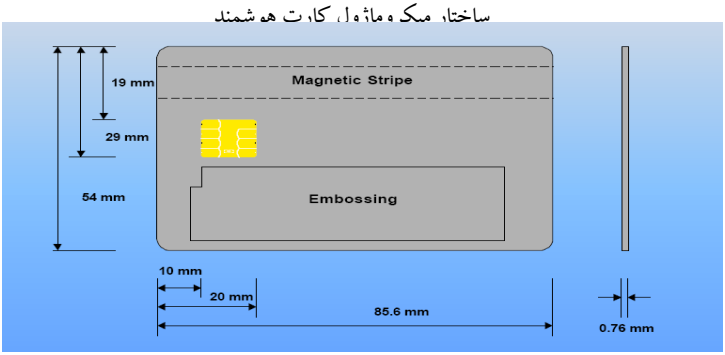
[۲] Microcontact

[۳] Microchip

ریزپردازنده یا واحد پردازشگر[۱] صادر می‌کند. واحد پردازشگر نیز دستورالعمل‌های برنامه‌ریزی شده را اجرا می‌کند. ریزپردازنده، مغز کارت هوشمند محسوب می‌شود.



ساختار میکرو ماژول کارت هوشمند



یک نمونه کارت هوشمند در ابعاد کارت های اعتباری، مطابق با استاندارد ISO/IEC ۷۸۱۰

کارت‌های هوشمند، علی‌رغم کوچک بودن تقریباً کلیه اجزای یک سیستم کامل کامپیوتری مانند ورودی و خروجی، CPU و انواع مختلف حافظه را دارا هستند. همه این قسمت‌ها در ریزتراشه (میکروکنترلر) تعبیه شده است. با تجمع ریزپردازنده و حافظه در

[۱] MPU: MicroProcessor Unit

یک ریزتراشه، امنیت بالا می‌رود چراکه پی‌بردن به اینکه چه ارتباطی بین این دو در حال رخ دادن است بدون استفاده از ابزار جستجوگر خاص، بسیار سخت است. ریزپردازنده از مجموعه دستورالعمل‌های محدود کننده ای مانند رمزنگاری برای برنامه‌های کاربردی استفاده می کند.

به واسطه محدودیت‌هایی که در سایز تراشه‌های کارت‌های هوشمند وجود دارد و همچنین تمایل به کوچک بودن این تراشه‌ها، محدودیت‌هایی در توابع و منابعی که می‌توانند در آن گنجانده شوند، وجود دارد.

چندین دلیل برای محدودیت در اندازه تراشه‌ها وجود دارد:

۱. هزینه‌ای که یک تراشه دارد، متناسب با مساحت سیلیکونی است که به آن اختصاص داده شده است.

۲. اغلب کارت‌های هوشمند، توسط پست معمولی تحویل داده می‌شوند؛ بنابراین می‌بایست در برابر تا شدن، پیچاندن و... مقاوم باشند. اگر تراشه خیلی بزرگ باشد، این فشارها ممکن است که تراشه، اتصالات (سیم‌های) بین تراشه و سطح یا آنتن را بشکنند.

۳. هرچه تراشه بزرگتر و پیچیده‌تر باشد نیاز به برق بیشتری خواهد داشت. دستگاه‌های کارت‌خوان معمولاً در تأمین جریان

برق، خسیسانه عمل می‌کنند؛ علاوه بر این مسأله اتلاف دما در داخل ماژول نیز مطرح است.

حافظه استفاده شده در کارت می‌تواند به سه قسمتRAM، ROM و حافظه غیرفرار یا NVM[۱] تقسیم شود. اطلاعات موجود بر روی ROM فقط یکبار و آن هم در هنگام تولید، نوشته می‌شود. از ROM برای ذخیره سیستم‌عامل و نگهداری طولانی مدت داده استفاده می‌شود. هنگام استفاده از کارت های هوشمند، برنامه‌های کاربردی در RAM اجرا می‌شوند. با قطع برق، کلیه محتویات RAM از دست می‌رود، بنابراین داده‌هایی که می‌بایست محفوظ بمانند، نباید در RAM ذخیره شوند. از RAM برای ذخیره برنامه‌های اجرا شده و داده‌های موقت استفاده می‌شود.

این مشکل با استفاده از NVM حل می‌شود، چرا که محیطی از حافظه را فراهم می‌کند تا داده‌ها به صورت دایم ذخیره شوند. نوع معمول NVM که بیشتر استفاده می‌شود EEPROM[۲] یا یک Flash EEPROM است، که اجازه می‌دهد داده‌ها به صورت دراز مدت ذخیره شوند و قابل تغییر نیز باشند. از این قسمت حافظه که می‌تواند بعد از تولید از کارخانه برنامه‌ریزی شود، برای ذخیره محتویات

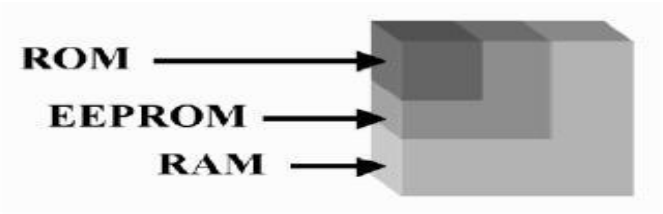
---

[۱] Non-Volatile Memory

[۲] Electronically Erasable-Programmable Read Only Memory

پایگاه داده، مانند اطلاعات تعیین هویت کاربر، ذخیره حافظه نهانی، اطلاعات گذشته کاربران واطلاعاتی از این دست استفاده می‌شود.

حافظه Flash نوع دیگری از انباره[۱] شناخته شده است که علی‌رغم مشهور بودن، استفاده از آن در کارت‌های هوشمند خیلی مرسوم نیست. به نظر می‌آید که این وضعیت در حال تغییر



مقایسه مساحت تراشه مورد نیاز برای هر یک از انواع حافظه

باشد و Flash بتواند به یک نوع حافظه برتر در کارت هوشمند تبدیل شود. این حافظه در برابر EEPROM مزایایی دارد که تمایل به سمت آنرا بیشتر می‌کند. اولاً اینکه EEPROM عمری محدود دارد و فقط امکان نوشتن تعداد معینی دفعه بر روی آن وجود دارد (کمتر از ۱۰۰۰۰۰ بار)؛ که این امر می‌تواند عمر برنامه‌های کاربردی یک کارت معین را محدود کند. حافظه Flash این مشکل را ندارد، ضمناً عملیات نوشتن روی آن نیز سریعتر می باشد. موضوع امنیت در این نوع حافظه دغدغه تولیدکنندگان کارت‌های هوشمند است.

---

[۱] Storage

حافظه کارت هوشمند به سه ناحیه با سطح دسترسی مختلف دسته‌بندی می‌شود. این نواحی شامل سه ناحیه تولیدکننده[۱]، ناحیه محرمانه[۲] و ناحیه وضعیت[۳] می باشد.

داده‌هایی مانند شماره‌ی ID کارت در ناحیه تولید کننده ذخیره می‌شود. این اطلاعات در هنگام تولید کارت در این ناحیه نوشته می‌شود و تنها CPU اجازه دسترسی به این ناحیه را دارد. ناحیه محرمانه، اطلاعاتی مانند کد شناسایی کاربر[۴] و کلید صادرکننده[۵] کارت را در بردارد. صادرکننده کارت، CPU و کاربر در صورت ارائه کلیدهای شناسایی درست و انجام فرایند هویت‌شناسی، مجاز به خواندن و نوشتن در این قسمت هستند. ناحیه وضعیت بخشی از حافظه است که تعداد دفعات تلاش برای دستیابی به کارت را حفظ می‌کند. بعد از تعداد معینی تلاش ناموفق برای دستیابی، کارت به صورت خودکار قفل شده و یا داده‌های مهم را از بین می‌برد.

❖ **سیستم‌عامل کارت هوشمند**

---

[۱] Manufacturer Zone

[۲] Secret Zone

[۳] Status Zone

[۴] PIN Code

[۵] Issuer

در حال حاضر کارت‌های هوشمند تقریباً یک کامپیوتر کامل بدون نمایشگر و صفحه کلید هستند. هسته مرکزی کارت هوشمند، یک ریزپردازنده است که قادر است سلسله دستوراتی را که به آن داده می‌شود اجرا نماید. این سلسله دستورات کارایی کارت را مشخص می‌کند. جهت مدیریت و اجرای این دستورات، مجموعه‌ای از توابع سطح بالا درون حافظه کارت ریخته می‌شوند. مجموعه این توابع را که به صورت دائمی درون حافظه کارت نوشته می‌شوند سیستم‌عامل کارت گویند. بنابراین سیستم‌عامل تراشه کارت هوشمند (COS[1]) یا Mask، رشته‌ای از دستورالعمل‌ها است که به طور ثابت در ROM کارت هوشمند قرار داده می‌شود. سیستم‌عامل، ریزپردازنده را قادر می‌سازد تا حافظه برنامه کاربردی را مطابق با فرامینی که توسط کاربر و از بیرون به کارت ارسال می‌شود، مدیریت و کنترل نماید. همچنین سیستم‌عامل، تأمین امنیت داده‌های روی کارت نیز به عهده دارد؛ به عنوان مثال تبادل امن داده‌ها بین کارت و سیستم میزبان و کنترل دسترسی به حافظه.

انواع کارت های هوشمند براساس سیستم‌عامل، عبارتند از:

- کارت‌های Open-OS
- کارت‌های Native (کارت‌های با OS خاص)

[1] COS: Chip Operating System

کارت‌های Open-OS دارای سیستم‌عامل‌هایی هستند که در سراسر جهان به عنوان استاندارد شناخته شده است. این کارت‌ها به Open Smart Card نیز معروف هستند. برخی از آنها عبارتند از:

- کارت‌های جاوا[۱]
- کارت‌های MULTOS[۲]
- کارت‌های هوشمند ویندوز[۳]

کارت‌های Native، سیستم‌عامل مشخص و استانداردی ندارند. سیستم‌عامل در این کارت‌ها شبیه OS بوده و توسط شرکت‌های مختلف با زبان‌های مختلف برنامه‌نویسی و یا با اسکریپت‌های خاص آن شرکت پیاده‌سازی می‌گردد. به همین دلیل امنیت نسبتاً خوبی را ارائه می‌دهد.

با توجه به خصوصی بودن سیستم‌عامل این دسته از کارت‌ها، توسعه نرم‌افزار و برنامه کاربردی برای آن ها بسیار مشکل است.

بیشتر سیستم‌عامل‌های کارت هوشمند از فایل سیستم مبتنی بر استاندارد ISO۷۸۱۶ پشتیبانی می‌کنند. سیستم‌عامل‌های کارت هوشمند از انجام عملیات معمول بر روی فایل‌ها مانند تولید، حذف، خواندن و نوشتن، و بروزرسانی فایل‌ها بر روی تمام فایل‌ها حمایت

---

[۱] Sun Micro System Java Technology

[۲] Multi Application Operating System

[۳] Microsoft Windows for Smart Cards

می‌کنند. هر فایل یک کارت هوشمند یک لیست کنترل دسترسی دارد؛ در این لیست مشخص می‌شود که چه موجودیتی اجازه اجرای چه عملیاتی را بر روی فایل خواهد داشت.

۱. سیستم‌عامل جاوا

این سیستم عامل اجازه می‌دهد برنامک‌های[۱] جاوا مستقیماً روی کارت‌های سازگار با استاندارد ISO۷۸۱۶ اجرا شوند. کارت‌های جاوا می‌توانند برنامه‌های کاربردی مختلف را به صورت مستقل از تراشه، اجرا نمایند. مدیر امنیت این کارت‌ها اجازه اجرا شدن برنامک را روی کارت صادر می‌کند.

۲. سیستم‌عامل MULTOS

سیستم‌عامل MULTOS، که توسط mondex International ایجاد شد، یک سیستم‌عامل باز چند کاربردی است که امنیت بالاتری نسبت به جاوا کارت ها فراهم می آورد. این سیستم‌عامل، امکان نگهداری همزمان چندین برنامه کاربردی مختلف بر روی کارت را فراهم می‌کند. مهمترین خصوصیت MULTOS عدم

[۱] Applets

وابستگی آن به زبان است. MULTOS تنها زیرساختی است که دارای یک زبان اسمبلر آسان ویک کامپایلرC است.کارت‌های جاوا و MULTOS هر دو می‌توانند جاوا را پشتیبانی کنند. در هر دو مورد یک کامپایلر جاوا، کد منبع[۱] را به کلاس جاوا ترجمه می‌کند.

۳. کارت‌های ویندوز

این سیستم‌عامل هشت بیتی و چند کاربردی، به هشت کیلو بایت ROM نیاز دارد. این سیستم‌عامل به گونه‌ای طراحی شده است که زیرساختی با قیمت پایین و آسان برای برنامه‌ریزی باشد و بتواند برنامه‌های کاربردی ویژوال بیسیک را اجرا نماید.

❖ **نرم‌افزار کارت هوشمند**

دو نوع نرم‌افزار کارت هوشمند وجود دارد:

۱. نرم‌افزار میزبان

نرم‌افزار میزبان بر روی کامپیوتری که به کارت هوشمند متصل است، نصب و اجرا می‌شود. اغلب نرم‌افزارهای کارت هوشمند، نرم‌فزار میزبان هستند؛ این نرم‌افزارها برای کامپیوترهای شخصی و

[۱] Source

کارگزارهای ایستگاه کاری[۱] نوشته می‌شود تا به کارت‌های هوشمند موجود دسترسی پیدا کرده و کارت‌ها را با سیستم‌های بزرگتر ترکیب نمایند. نرم‌افزار میزبان معمولاً شامل نرم‌افزارهای برنامه کاربردی و نرم‌افزار سیستم است.

۲. نرم‌افزار کارت

نرم‌افزار کارت، نرم‌افزاری است که بر روی خود کارت هوشمند اجرا می‌شود. این نرم‌افزار نیز شامل نرم‌افزار سیستم و نرم‌افزار برنامه‌ی کاربردی است. نرم‌افزار سیستم معمولاً شامل سیستم‌عامل و قابلیت‌هایی است که می‌تواند مدیریت حافظه را کنترل ، ارتباطات ورودی وخروجی با میزبان را راه‌اندازی و اطمینان در تبادل صحیح داده و امنیت آن را فراهم کند. برنامه کاربردی کارت که حاوی داده است، می‌تواند از توابعی که بر روی داده کار می‌کنند، پشتیبانی نماید.

❖ **زیرساخت ارتباطاتی کارت هوشمند**

یک کارت هوشمند برای ارتباط با دنیای خارج، باید درون یا نزدیک یک دستگاه کارت‌خوان قرار گیرد. با استفاده از این کارت‌خوان، علاوه بر خواندن اطلاعات کارت، می‌توان داده‌های آن را نیز تغییر داد. کارت هوشمند و دستگاه پذیرش کارت[۲] از

---

[۱] Workstation Servers

[۲] CAD

طریق بسته‌های کوچک داده، با یکدیگر ارتباط برقرار می‌کنند. ویژگی‌های ارتباط کارت هوشمند و دستگاه پذیرش کارت عبارتند از:

- نرخ بیت کم (۹۶۰۰ بیت بر ثانیه) با استفاده از یک خط ارتباطی سریال دو جهته،
- استفاده از مد نیمه دوطرفه[۱] برای ارسال داده‌ها روی این خط ارتباطی،
- استفاده از یک پروتکل خاص برای ارتباطات،

کارت‌ها از نظر متد ارتباطی با کارت خوان به سه دسته کارت‌های تماسی، غیرتماسی و ترکیبی تقسیم می‌شوند. آنچه در همه این متدها مشترک است، این است که برقراری ارتباط باید از طریق یک دستگاه کارت‌خوان و بر مبنای یک پروتکل ارتباطی صورت گیرد.

کارت هوشمند از هر نوعی که باشد، باید از طریق یک دستگاه کارت‌خوان با بیرون ارتباط برقرار کند. دستگاه کارت‌خوان یک لینک ارتباطی بین کارت و سیستم میزبان ایجاد می‌کند. سیستم میزبان می‌تواند یک کامپیوتر یا یک دستگاه مستقل باشد. کارت‌خوان توان الکتریکی مورد نیاز کارت را تامین می‌کند،

---

[۱] Half-duplex

کارت را مقداردهی اولیه می‌کند و به عنوان واسطه‌ای بین کارت و میزبان عمل می‌کند. مقداردهی اولیه، پروتکل تعریف شده‌ای است که در مورد تمام کارت‌ها باید انجام گیرد.

چند نمونه کارت خوان تماسی

❖ هویت‌شناسی و رمزنگاری

دستگاه‌های بیرونی که با کارت ارتباط برقرار می‌کنند، آن را در مقابل حملاتی از ناحیه ارتباط، آسیب‌پذیرتر می‌نمایند. لذا برای کاهش این تهدیدات، از مکانیزمی تحت عنوان هویت‌شناسی[۱] استفاده می‌شود. هویت‌شناسی، پروسه‌ای است که طی آن کارت، هویت طرف مقابل را که سعی در برقراری ارتباط با کارت دارد، شناسایی می‌کند. در این پروسه پیامی از طرف کارت به دستگاه بیرونی ارسال می‌شود، دستگاه بیرونی آن را بوسیله کلید خود، رمز می کند و پیام رمز شده را به کارت بر می‌گرداند. کارت این پیام را با کلید خودش رمزگشایی می‌کند و آن را با پیامی که به بیرون ارسال کرده بود، مقایسه می‌کند. در صورتی که هر دو پیام با

[۱] Authentication

هم تطابق داشته باشد، هویت آن موجودیت برای کارت محرز می‌گردد، هویت‌شناسی می‌تواند دو طرفه انجام شود.

هنگامی که ارتباط برقرار شد، پیام‌های مبادله شده بین طرفین، از طریق یک کد تحت عنوان کد احراز هویت پیام، ارزیابی می‌گردند. این کد بر اساس خود داده‌ها، یک کلید رمزنگاری و یک عدد تصادفی، محاسبه می‌گردد. در صورتی که داده‌ها به هر دلیلی (مثل خطای ارسال) تغییر نمایند، باید دوباره ارسال گردند.

در صورتی که تراشه روی کارت حافظه و قدرت پردازشی کافی داشته باشد، داده‌ها می‌توانند از طریق یک امضای دیجیتال نیز ارزیابی گردند.

یکی دیگر از اقدامات امنیتی بر روی ارتباطات کارت با دنیای بیرون،رمز نمودن پیام‌هایی است که بین کارت و دنیای بیرون کارت مبادله می‌شود. سیستم رمزنگاری مبتنی بر کارت هوشمند نیز شبیه سایر سیستم‌های رمزنگاری است.

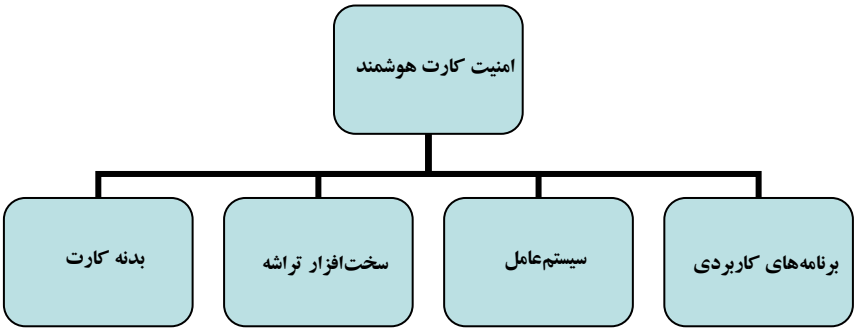
❖ **استانداردهای کارت های هوشمند**

در ادامه به استانداردهای مطرح امنیتی در خصوص کارت های هوشمند و حوزه های تحت پوشش آن ها نگاهی اجمالی خواهیم داشت.

	ISO ۷۸۱۰/۷۸۱۳	ISO ۷۸۱۶-x	FIPS ۱۴۰-۲	SCSUG-SCPP
بدنه کارت	*			
امنیت فیزیکی کارت			*	*
امنیت سیستم عامل کارت		*	*	*
امنیت نرم‌افزار کارت		*	*	*
ساختار اشیاء داده‌ای امن		*		
روش مقاومت در برابر حملات مختلف			*	*
امنیت رمزنگاری			*	*
سیاست‌گذاری‌های امنیتی			*	*
امنیت پروتکل ارتباطی		*	*	*
مدیریت کارت		*	*	
روش‌های بیومتریک		*		

فصل ٤ - ملاحظات پدافند غیرعامل در طراحی کارت هوشمند

موضوع امنیت، ایمنی و پایداری نقطه عطف اصلی در استفاده از این کارت ها می باشد؛ از اینرو در این فصل نگاهی اجمالی به نیازها و ویژگی های امنیتی مورد نیاز در طراحی یک کارت هوشمند در جهت مصونیت از خطرات متصور در فضای جنگ سایبر و مخاصمات بین الملل خواهیم داشت.

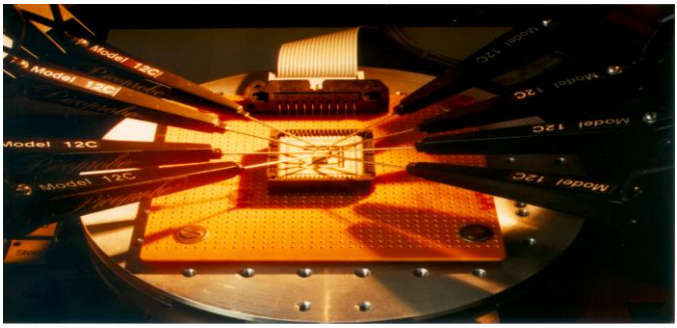


- طراحی کارت هوشمند در هنگام توسعه می بایست شامل یک مکانیزم امنیتی بومی و منتشرنشده باشد که تنها طراح از آن مطلع است و این مکانیزم از دیدگاه طراح به عنوان شرط تضمین کننده برقراری امنیت کارت هوشمند منظور گردد.

- هیچ کدام از باس های درونی تراشه که پردازنده را به حافظه های ROM ، RAM و EEPROM متصل می سازند، نباید بیرون از تراشه قرار گیرند و نباید امکان برقراری هیچ گونه اتصال مستقیمی از بیرون به این باس ها وجود داشته باشد.
- از آنجا که در حال حاضر به علت محدودیت های موجود، امکان تولید تراشه در داخل کشور مقدور نمی باشد و با توجه به تهدیدهایی نظیر آنچه که در جنگ های اطلاعاتی روی می دهد و یا دیگر برنامه های تخریبی دشمنان، جهت عدم وابستگی به یک فراهم کننده ماژول کارت هوشمند، باید حداقل از چند فراهم کننده مختلف که تأمین کننده نیازهای امنیتی ماژول مورد نظر باشند استفاده نمود؛ تا در صورت اعمال تحریم توسط یک فراهم کننده برای کشور، نسبت به آن فراهم کننده وابستگی بوجود نیاید و بتوان ماژول های تهیه شده از فراهم کنندگان دیگر را جایگزین ماژول فعلی نمود؛ هرچند رویکرد بهینه برای مرحله تولید کارت، انتقال فناوری تولید و ساخت تراشه های کارت هوشمند در داخل کشور است.
- یک کارت هوشمند نیاز به مکانیزمی برای تشخیص حمله دارد تا در مواقع لزوم در برابر آن واکنش نشان داده و به طور مثال کلیدهای محرمانه را پاک نماید؛ این مکانیزم می تواند توسط

پروسه ای که غیر از شرایط نرمال عملکرد باشد ایجاد شود؛ بطور مثال ولتاژ بالاتر و یا تغییر نرخ کلاک پالس[۱]؛ از آنجایی که این شرایط در زمانی که خطایی در سامانه اتفاق بیافتد نیز ممکن است رخ دهد، معمولاً از مکانیزم اتوماتیکی برای بلوکه و یا پاک کردن کلیدها استفاده نمی شود؛ مگر در کاربردهای خاص استفاده از کارت هوشمند در حوزه های سری و خیلی محرمانه.

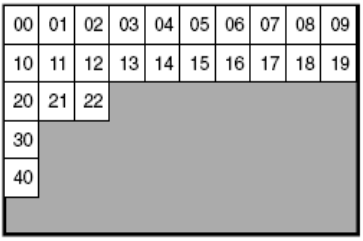
- در طراحی یک ماژول کارت هوشمند در سطح ملی، بایستی از ماژول چند لایه استفاده شده و در لایه فوقانی و تحتانی آن نباید اطلاعات ذخیره شود. این عمل در جلوگیری از دسترسی به محتویات داخلی حافظه کارت بخصوصEEPROM تأثیر بسزایی خواهد داشت.

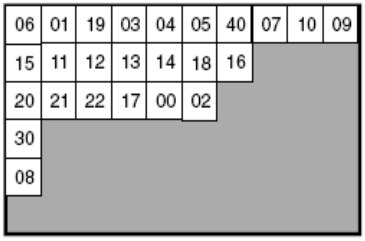


تحلیل ریزتراشه توسط پراب‌گذاری

[۱] Clock pulse

- اندازه های ساختاری فناوری نیمه هادی بکار رفته در سخت افزار تراشه در حدود یک میکرومتر در نظر گرفته شود.
- طراحی مدارهای مجتمع نیمه هادی تراشه شامل پردازنده و حافظه ها باید به گونه ای ویژه و جدا از روال های مرسوم طراحی در نظر گرفته شوند.
- جهت ایجاد مانع برای اسکن تراشه به منظور تعیین جزئیات آن، می بایست از لایه هایی فلزی در طراحی تراشه استفاده نمود.
- در هنگام طراحی بر روی سطح تراشه می بایست لایه های فلزی برای توزیع توان در نظرگرفته شوند.
- می بایست در کنار RAM از حسگری دمایی استفاده شود تا در صورت تغییر ناگهانی یا پایین آمدن بیش از حد مجاز دما، کلیدهای سری پاک شود. همچنین می بایست مکانیزمی برای پاک شدن محتویات، در صورت مقیم شدن طولانی مدت کلیدها یا پارامترهای سری، درون RAM وجود داشته باشد.
- فضای آدرس دهی سلول های حافظه درون تراشه با یک طرح درهم ریختگی منحصر به تراشه می بایست پیچیده سازی شود بنابراین حافظه EEPROM می بایست با یک طرح درهم ریختگی به طور نرم افزاری آدرس دهی شود. در کنار درهم ریختگی می توان از رمزگذاری حافظه نیز استفاده نمود.





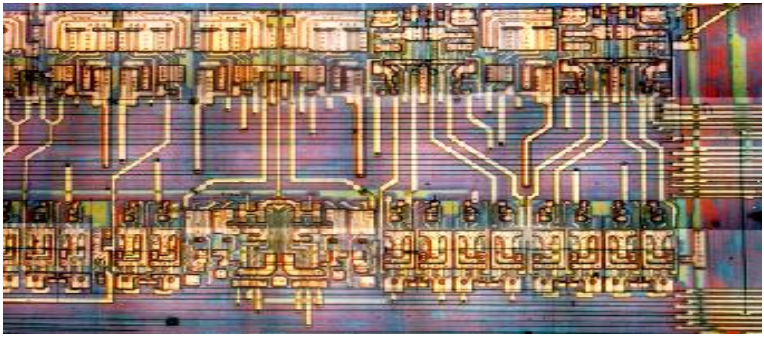
پیچیده نمودن حافظه

- برای رمزگذاری فضای آدرس دهی سلول های حافظه می بایست از الگوریتم رمز بومی و قدرتمند استفاده نمود.
- ماژول مورد استفاده در کارت هوشمند ملی بایستی دارای حسگر نوری جهت تشخیص نفوذ و حمله فیزیکی به تراشه باشد و در صورت حمله، بایستی اقدامات لازم جهت جلوگیری از دسترسی مهاجم به اطلاعات حساس پیش بینی شده باشد.
- تراشه می بایست مجهز به یک مدار ناظر بر ولتاژ باشد تا در صورتی که ولتاژ تراشه از محدوده تعریف شده تجاوز نمود، آن را خاموش نماید.
- تراشه می بایست مجهز به مداری جهت نظارت بر فرکانس عملکرد تراشه باشد تا اگر فرکانس از نرخ کلاک تعریف شده کمتر یا بیشتر شد، عکس العمل نشان دهد.

- باس های درونی متصل به حافظه می بایست با یک طرح منحصر به تراشه درهم ریخته شوند.

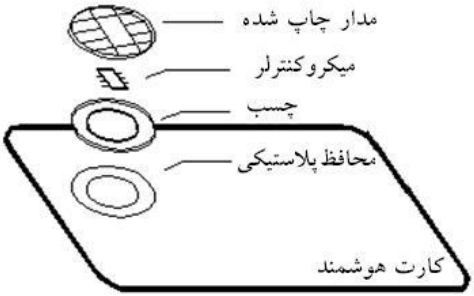
پیچیده نمودن باس داده

- در برنامه ریزی تراشه می بایست دستورالعمل هایی با مصارف یکسان جریان به کارگیری شود .
- در کد اسمبلی نباید از دستورالعمل هایی که مصرف آنها با سطح میانگین تفاوت معنی داری دارد، استفاده شود.
- در الگوریتم رمز می بایست از چندین پروسه متفاوت برای اجرای محاسبات مشابه استفاده نمود.
- تراشه می بایست مجهز به رگولاتورهای ولتاژ سریع باشد تا جریان های مصرفی درون تراشه را یکسان سازی نماید. در صورت مجهز نبودن تراشه به رگولاتورهای ولتاژ سریع می بایست در درون آن مولدهای نویز مصنوعی تعبیه شده باشد تا توان مصرفی تراشه را یکنواخت نمایند.



لایه درونی تراشه زیرمیکروسکوپ

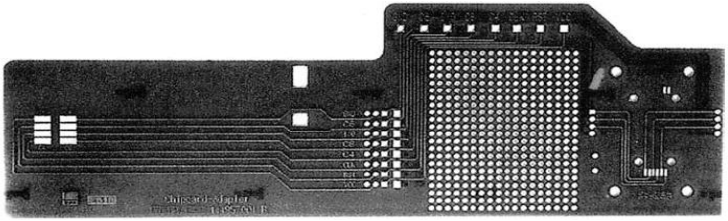
- وجود مقاومت حسگر برای تنظیم جریان مصرفی به صورت مستقل از دستورالعمل های اجرا شده، موجب جلوگیری از حملات توان مصرفی در صورت اجرای دستورالعمل های مختلف می گردد.
- تمهیدات و مکانیسم های امنیتی در نظر گرفته شده برای برنامه های کاربردی مختلف باید با توجه به ملزومات امنیتی آنها تعریف شود.
- بجز در موارد الزامی و مشخص، دسترسی به منابع و فایل ها در کارت هوشمند، بایستی محدود شود و سطوح دسترسی بایستی بصورت مشخص در مستندات آورده شود.
- بمنظور افزایش سطح امنیت، بایستی ارزیابی کارت در سطوح مختلف امکان پذیر باشد و نباید کلیه کلیدهای مورد نیاز جهت ارزیابی را تنها در یک پایانه نگهداری نمود.



اجزای تشکیل دهنده کارت هوشمند

- می بایست تمهیدات لازم جهت بازگشت خودکار سامانه کارت به حالت اولیه در صورت بروز خطا پیش بینی گردد.
- لازم است برای افزایش ضریب امنیت، تصدیق اصالت دوطرفه صورت گیرد و همچنین اصالت کارت توسط پایانه و هم اصالت پایانه توسط کارت بررسی شود.
- در صورتی که ارتباط برخط برای هر تراکنش در کارت امکان پذیر نباشد بایستی محدودیت هایی برای حداکثر میزان تراکنش های برون خط برای یک پایانه و یک کارت در نظر گرفت.
- روتین دستورات و کلاس دستورالعمل های درون نرم افزار کارت نباید آشکار و عمومی یا قابل بازیابی توسط روال های کشف دستورالعمل ها باشد .

- بمنظور جلوگیری از بهره برداری از داده های در حال عملکرد می بایست از ترمینال هایی که توسط دیافراگم هایی اجازه اتصال سیم های اضافی به کارت را نمی دهند و یا مکانیزم پیام رسانی امن استفاده نمود.



آداپتور انتقال داده‌ها

- روتین نرم افزاری مقایسه PIN باید به گونه ای باشد که تمامی ارقام آن را به یکباره مقایسه نماید.
- اجرای مکانیزم های امنیتی نظیر رمزنگاری و احراز هویت می بایست مستقل از زمان پردازش داده ها وکلیدهای مختلف باشد تا حملات زمانی که با تحلیل زمان اجرای داده های مختلف کلید را حدس می زنند، قابل اجرا نباشد.
- الگوریتم های رمزنگاری بکاررفته باید عاری از نویز و مستقل از طول داده ها یا کلید های مختلف باشند.
- فلوچارت برنامه های نرم افزاری باید بسیار قوی طراحی شده باشد . برای این منظور در صورتیکه در بخش هایی از فلوچارت تصمیم گیری مورد نیاز باشد، می بایست برای هر یک از حالات

ممکن برای یک شرط دستورالعملی به صورت مجزا وجود داشته باشد.

- حسگرهای آشکارساز پالس های ولتاژ و یا نور ناگهانی می توانند در تشخیص حمله هایی که با ایجاد خطا در عملکرد پردازنده و مشغول نمودن آن موجب عدم پایداری پردازنده می گردند، نقش موثری داشته باشند.
- بهتر است از یک سیستم عامل بومی جهت استفاده در سامانه کارت هوشمند استفاده شود؛ لیکن در صورت عدم دسترسی به سیستم عامل بومی که دارای قابلیت های مورد نظر باشد، می توان بخشی از سیستم عامل های موجود را بومی سازی و از الگوریتم های اختصاصی برای قسمت های حساس سیستم عامل استفاده نمود.
- لازم است تمامی ارتباطات حساس کارت با ترمینال از جمله روال های احراز هویت توسط برنامه های رمزنگاری و با طول کلید سری مناسب رمز شوند.
- ثبات ها و شمارنده هایی که در برنامه، وظیفه نشان دادن اجرای عملی را دارند باید به گونه ای مخفی سازی شوند تا با بررسی آنها عمل انجام شده مشخص نباشد.

- می بایست طبق استاندارد خاصی ترتیب قرار گرفتن دستورالعمل در EEPROM پشت سر هم و با دقت صورت گیرد تا قطع توان باعث اجرا نشدن بخش امنیتی برنامه نشود.
- کارت هوشمند را باید بتوان در انتهای چرخه حیات به صورت کامل توسط سیستم عامل، غیر فعال نمود؛ اطلاعات غیر ضروری در پایان چرخه حیات کارت بایستی بطور کامل حذف گردند.