موضوع پروژه:

کارت هوشمند

سرفصل مطالب

دیباچه

آنچه در پی می آید، مجموعه مطالبی است که پس از تحقیق و بررسی فراوان از میان منابع مختلف بدین شکل گردآوری شده است. کلیه مطالب در ارتباط با کارت هوشمند در پنج فصل گردآوری شده است تا خواننده علاقه مند به مطالب، پس از مطالعه به یک اشراف کلی در مورد کارت هوشمند دست یابد.

مطالب مطروحه به نحو ساده ای بیان شده اند و برای تفهیم به پیش نیاز خاصی احتیاج نمی باشد . تلاش بر این بوده است تا با رعایت سیر منطقی بیان مطالب، مطالب خاصی ناگفته باقی نماند وخواننده به درکی وسیع (و نه الزاما عمیق!) درباره ی کارت هوشمند برسد.

در فصل اول در مورد خصوصیات فیزیکی یک کارت و ویژگی های تراشه و استانداردهای موجود و تکنولوژی های مرتبط صحبت می شود.

در فصل دوم اجزاء و مولفه های یک سیستم کارتی هوشمند مورد بحث و بررسی قرار خواهند گرفت.

فصل سوم اختصاص به ساختار مدیریت چرخه دوام کارت دارد.

در فصل چهارم امکانات کارت های هوشمند برای استفاده در آژانس ها مورد بررسی قرار گرفته است.

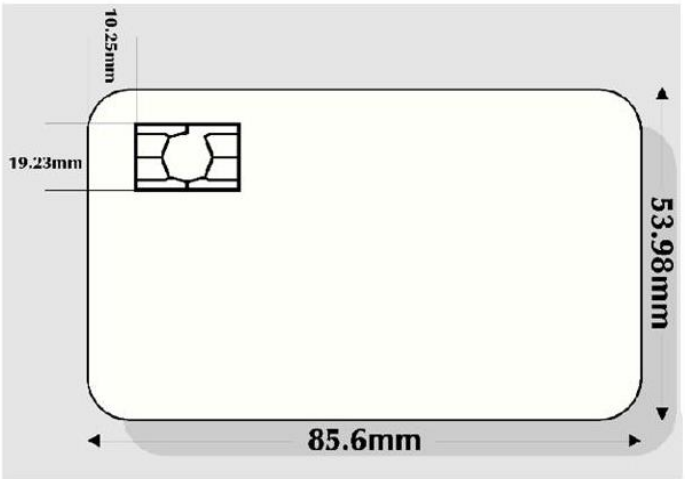
و در نهایت فصل پنجم اختصاص به مزایای نسبی کارت های هوشمند در مقایسه با دیگر تکنولوژی های مرتبط دارد.

فصل اول – مقدمه ای بر کارت های هوشمند (introduction to smart cards)

واژه ی کارت هوشمند از لحاظ ظاهری پر طمطراق و از لحاظ مفهومی نیز بسیار مبهم است و به شکل های گوناگون از این واژه استفاده می شود . سازمان بین المللی استانداردها[1] از واژه ی کارت های مدار مجتمع[2] استفاده می کند که شامل وسایلی می شود که در آن ها یک مدار مجتمع در داخل یک کارت شناسایی پلاستیکی که دارای استاندارد ISO 1 است کار گذاشته شود . این کارت در ابعاد ۸۵,۶*۵۳,۹۸ * ۰,۷۶ میلیمتر مانند کارت های بانکی که دارای نوار مغناطیسی هستند ساخته می شود .

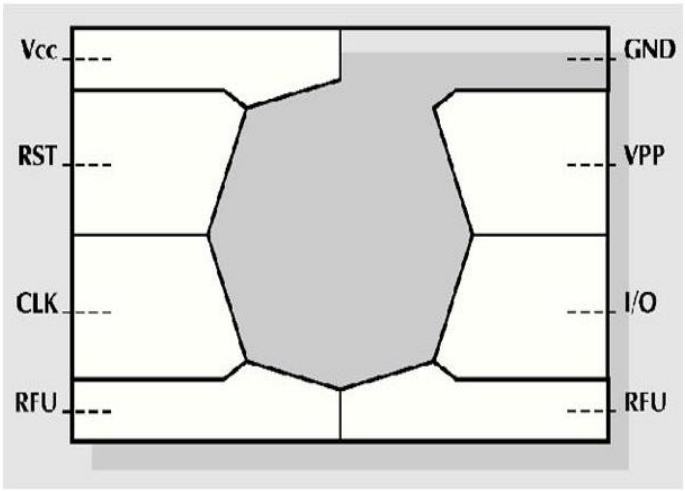
کارت های مدار مجتمع در دو شکل تماسی[3] و بدون تماس[4] موجود می باشند . نوع تماسی به سادگی بوسیله کانکتور طلایی رنگ قابل تشخیص می باشد.

گرچه استاندارد ایزو (۲-۷۸۱۶) ، ۸ کنتاکت را تعریف می کند، ولی در واقع فقط ۶ کنتاکت از ۸ کنتاکت برای ارتباط با دنیای خارج به کار گرفته می شوند. . کارت های بدون تماس ممکن است دارای باتری باشند خصوصا در نوع super smart cards که دارای صفحه کلید مجتمع و صفحه نمایش LCD می باشند. به طور کلی نیروی عامل برای کارت های بدون تماس الکترونیکی بوسیله حلقه ی القایی که از پرتوی الکترومغناطیسی فرکانس پایین استفاده می کند ، تامین می شود به همین شکل سیگنال ارتباطی مخابره می شود و یا می توان از کوپلینگ خازنی و یا حتی ارتباط بصری استفاده کرد .



[1] - International Standards Organization (ISO)
[2] - Integrated Circuit Cards (ICC)
[3] - Contact Card
[4] - Contactless Cards

کارت های تماسی بخاطر استفاده گسترده از آن ها به عنوان یک کارت پیش پرداخت تلفنی در فرانسه و در اکثر کشورهای اروپایی رایج ترین ICC موجود بودند . بیشتر کارت های تماسی شامل یک مدار مجتمع ساده می باشند ، گرچه در بعضی از تجربه های آزمایشی از دو تراشه استفاده می شود . تراشه به تنهایی میان سازندگان مختلف ، برای کاربردهای مختلف دارای انواع نسبتا زیادی است .



وظیفه ی Vcc تامین ولتاژ مورد نیاز برای به کار انداختن تراشه است که در گذشته Vcc معمولا ۵ ولت بود ولی امروزه تراشه ها با یک ولتاژ ۳ ولتی شروع به کار می کنند که این ولتاژ کمتر بواسطه پیشرفت هایی است که در تکنولوژی نیمه هادی ها بدست آمده است . Vss ولتاژ زمین مورد نیاز در برابر ولتاژ Vcc است. reset خط سیگنالی است که برای راه انداختن وضعیت مدار مجتمع بعد از روشن شدن به کار میرود . سیگنال ساعت[1] به عنوان، ولت محرک منطق مدار مجتمع به کار می رود و همینطور در نقش رابط ارتباط سری ظاهر میشود . دو سرعت متداول برای ساعت 3.57 MHz , 4.92 MHz است . در گذشته سرعت کمتر در اروپا رایج تر بوده است ولی امروزه تا اندازه ی زیادی محبوبیت خود را از دست داده است .

ممکن است این سوال پیش آید که چرا این فرکانس های نا آشنا انتخاب شده اند و چرا فرکانس سرراست 5 MHZ انتخاب نشده است . از هر دوی این فرکانس ها به عنوان فرکانس حاصل فرعی رنگی[2] در دنیای

[1] - clock signal
[2] - Colour sub carrier frequency

تلویزیون استفاده می شود . سیستم PAL برای فرمان دادن از فرکانس 4.92 MHZ استفاده می کند . در حالیکه فرکانس 3.57 MHZ بوسیله استاندارد NTSC آمریکا مورد استفاده قرار می گیرد .

کنتاکتور Vpp برای سیگنال ولتاژ بالا مورد نیاز که برای برنامه ریزی حافظه EPROM ضروری است به کار میرود . کنتاکتور IO خط سیگنالی است که بوسیله آن تراشه دستورات را دریافت و اطلاعات را با دنیای خارج مبادله می کند .

نخستین موارد استفاده از کارت های IC برای ذخیره ی اطلاعات قابل حمل و بازیابی آن ها بوده است . از این رو اجزای اصلی یک IC ماژول های حافظه هستند . لیست زیر انواع رایج تر حافظه را ارائه می کند .

- حافظه فقط خواندنی ROM
- حافظه فقط خواندنی قابل برنامه ریزی P ROM
- حافظه فقط خواندنی قابل برنامه ریزی و قابل پاک کردن EPROM
- حافظه فقط خواندنی قابل برنامه ریزی و قابل پاک کردن الکتریکی EEPROM
- حافظه با دستیابی تصادفی RAM

یک تراشه خاص ممکن است دارای یک یا تعداد بیشتری از انواع حافظه باشد . این حافظه ها هر یک دارای خصوصیات منحصر به فردی هستند . ROM نوعی از حافظه است که پس از ساخت بوسیله شرکت سازنده ، دیگر قابل تغییر نیست. این نوع حافظه قیمت پایینی دارد به این خاطر که حداقل فضا را در لایه ی سیلیکون اشغال کرده است .

مشکل اصلی ROM ، طولانی بودن فرآیند تولید آن و نیز تغییری ناپذیری پس از ساخت است . با توجه به این مشکلات و نیز میزان اندک سفارشات قیمت آن ها در مقایسه با دیگر حافظه ها بسیار پایین است .

حافظه ی P ROM بواسطه لنیکهای ذوب شونده ، بوسیله کاربر قابل برنامه ریزی است . اما برای عملیات برنامه ریزی نیاز به جریان ولتاژ بالا است و از چنین وسایلی معمولا در کارت های مدار مجتمع استفاده نمی شود .

EPROM ها در گذشته به طور گسترده مورد استفاده قرار می گرفتند اما چنین اسمی برای این کاربردها مناسب نبود . با وجود اینکه این حافظه بوسیله اشعه ماوراء بنفش قابل پاک شدن است در ICC دریچه کوارتنز لازم هیچ وقت در دسترس نیست حافظه یک بار قابل برنامه ریزی است از این رو به آنها OTP که مخفف one time programmable است نیز می گویند .

تحویل اساسی در EEPROM ها صورت گرفت. این حافظه توسط کاربر قابل پاک شدن بود و همینطور دفعات زیادی قابل نوشتن بود (بین ۱۰۰۰۰ تا ۱,۰۰۰,۰۰۰ مرتبه در کاربردهای معمولی) .

تمام حافظه هایی که تا کنون توصیف شدند غیر فرار بودند به عبارت دیگر هنگامی که ارتباط با منبع تجزیه از بین برود ، آنها محتویات خود را حفظ می کنند. در حافظه های RAM شرایط به گونه ای دیگر است . RAM یک نوع حافظه فرار است و به محض اینکه منبع نیروی لازم را تامین نکند ، اطلاعات از بین می روند. در فصل های بعدی به بررسی جزء به جزء هر یک از این حافظه ها می پردازیم .

برای ادامه بیشتر این بحث باید توجه داشته باشیم که حداکثر قیمت یک IC به میزان سیلیکون به کار رفته در آن بستگی دارد. کانکتور ایزو به شکلی طراحی می شود تا قطعات مستطیلی سیلیکون ابعادی به اندازه ۲۵ میلیمتر مربع داشته باشند.(گر چه امکان استفاده از ابعاد ۳۵ میلیمتر مربع یا بیشتر نیز وجود دارد) نکته حائز اهمیت مربوط به قابلیت اطمینان در برابر خطرات ناشی از شکستگی های مکانیکی است که در ابعاد بزرگتر ، بیشتر رخ می دهد. واضح است که به هرحال باید تلاش شود که حجم تراشه را کاهش داده تا هم از لحاظ قیمت و هم از لحاظ حجم متناسب با کاربرد خاص مورد نظر باشد.

گرچه کارت معمولی نیاز به یک حافظه EEPROM (128 B تا 512B) و منطق کنترل حافظه دارد ، برای کاربرد های پیچیده- تر وجود CPU , RAM , EEPROM, ROM برای انجام عملیات لازم و ضروری است. در واقع به کاربردن CPU یا ریزپدازنده است که منجر به استفاده از واژه «smart» می شود.

در منطق کنترل باید توجه شود که از این کارت ها هم درارتباطات مخابراتی و هم برای ایجاد روش هایی در جهت حفاظت از حافظه در برابر اعمال خلافکارانه استفاده می شود.

شاید ICC در واقع همان آرزوی دیرینه انسان ها بوده است که بر خلاف اکثر ذخیره کننده های الکترونیکی و ابزار پردازش در آنها مقوله امنیت لحاظ شده است. بنابراین امروزه ما می توانیم میان انواع مختلف ICC از لحاظ حجم (انباره) وامنیت تفاوت قائل شویم.

☐ فقط حافظه

☐ حافظه با منطق امنیت

☐ حافظه با CPU

از منطق امنیت می توان برای کنترل دسترسی به حافظه استفاده کرد. این دسترسی به حافظه را می توان بوسیله کد دسترسی که معمولاً کد بزرگی هم هست انجام داد (۶۴ بیت یا بیشتر). واضح است که استفاده از حافظه EEPROM باید به شکل سختگیرانه ای مورد کنترل قرار بگیرد. به این دلیل که افراد شیاد می توانند سودهای هنگفتی را با استفاده بدون مجوز از حافظه به جیب بزنند. در فصل های آتی در مورد مقوله امنیت به بحث بیشتری می پردازیم .

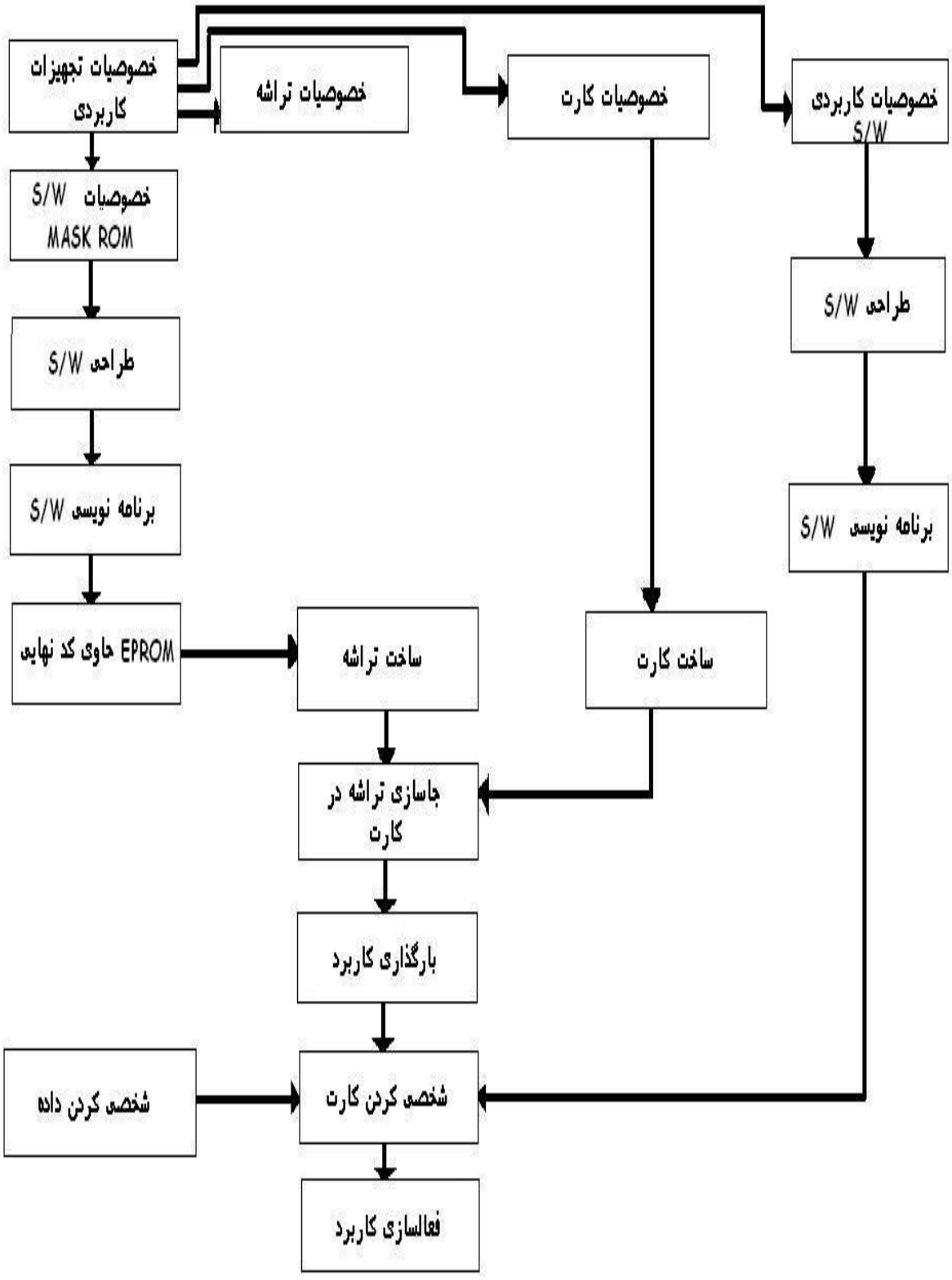
در دنیای کارت های هوشمند واژه «کاربرد»[1] به طور گسترده ای در توصیف نرم افزارها یا برنامه هایی که توسط IC انجام می شود به کار می رود. در ساده ترین شکل ، یک کاربرد ، مدیریت یک فایل برای

سازماندهی اطلاعات ذخیره شده یا دریافتی است. چنین کاربردی به طور کامل در منطق یک تراشه انجام می شود. به همین نحو یک تراشه باید دارای منطق ارتباط باشد که بوسیله آن دستورات توسط دستگاه پذیرنده کارت پذیرفته شوند و بواسطه آن اطلاعات کاربردی را دریافت و انتقال می دهد.

این ICC که دارای یک CPU می باشد، می تواند کاربردهای پیچیده ای را انجام داده و حتی کاربردهای چند گانه را نیز انجام دهد، زیرا CPU توانایی پردازش اطلاعات و تصمیم گیری روی عملیات مختلفی که ممکن است توسط کاربرد درخواست شده را دارد .

۱،۱) یک کارت IC چگونه ساخته می شود؟ (How the IC card is made?)

طراحی و ساخت یک کارت هوشمند شامل عملیات متعددی است که در آن ها چگونگی تعبیه و جاسازی تراشه بر روی کارت پلاستیکی در کیفیت محصول نهایی بسیار کلیدی است. عملیات تعبیه به ساختمان کارت بستگی دارد و کل عملیات به خصوصیات و نیازهای کاربرد بستگی دارد. برای ویژگی های مشخص باید به صورت مجزا تراشه ، کارت ، نرم افزار مربوط به ROM و نرم افزار کاربرد را تجهیز کرد.نرم افزار ROM توسط فروشنده نیمه هادی که تراشه را می سازد تهیه میشود. سازنده کارت، تراشه را روی کارت پلاستیکی قرار می دهد. پر واضح است که سازنده باید اطلاعات شخصی شده و نرم افزار کاربردی را بار گذاری کند. امنیت یکی از جنبه های اصلی در فرایند ساخت کار هوشمند و درتولید نهایی حیاتی است. به همین دلیل در ادامه و در فصل مقرر به بررسی جداگانه این مقوله می پردازیم شکل زیر مراحل ساخت یک کارت هوشمند را نشان می دهد .



شکل ۳. مراحل ساخت یک کارت هوشمند

۲,۱) خصوصیات تراشه (Chip specification)

چندین عامل برای تصمیم گیری در مورد ویژگی های مدار مجتمع برای استفاده در یک کارت هوشمند وجود دارد. برای مثال یک کارت CPU را در نظر می گیریم. ساخت یک کارت حافظه اساساً زیر مجموعه مواردی است که در ادامه می آید. پارامترهای کلیدی در مورد ویژگی ها و خصوصیات یک تراشه موارد زیر هستند .

- ☐ نوع ریزپردازنده
- ☐ سایز Mask ROM
- ☐ نوع حافظه غیر فرار (برای مثال EEPROM یا EPROM)
- ☐ اندازه حافظه غیر فرار
- ☐ سرعت ساعت (خارجی و گاهاً به صورت اختیاری داخلی)
- ☐ پارامترهای الکتریکی (ولتاژ و جریان)
- ☐ پارامترهای ارتباطی (همگام ، غیر همگام ، بایت ، بلاک)
- ☐ مکانیزم راه اندازی مجدد
- ☐ حالت Sleep (جریان کم و در انتظار عملیات)
- ☐ پردازشگر کمکی (برای مثال رمز نویسی کلید عمومی[۱])

از لحاظ عملی، کارخانه های سازنده نیمه هادی محدوده ای مشخص برای محصولات تولیدی خود دارند که در آن محدوده پارامترهایی که در بالا آمده است ، از پیشین تعیین و مشخص می شوند .

بنابراین وظیفه طراح انتخاب محصول مناسب برای کاربرد معین و مشخص است . همانطور که قبلاً اشاره شد " امنیت " از لحاظ عملی مقوله بسیار مهی است. بنابراین یک تراشه معین ممکن است نیاز به تجهیزات اضافی چه از لحاظ فیزیکی و چه از بابت تجهیزات منطقی داشته باشد .

ETSI (موسسه استاندارد مخابرات اروپائیان) استانداردهای جدیدی برای کمیته CEN TC224 وضع کرد. این استاندارد ها از استانداردهایی که ISO معین کرده است، بسیار دقیق تر هستند.

برای مثال ISO 7816-3 جریان کارت را تا ۲۰۰ میلی آمپر مجاز شمرده است ولی ETSI برای موارد معمولی ۲۰ میلی آمپر و برای کاربردی نظیر تلفن های همراه ۱۰ میلی آمپر را توصیه کرده است .

۳,۱) خصوصیات کارت (Card specification)

خصوصیات یک کارت شامل پارامترهایی رایج موجود در بسیاری از کاربردهایی که از کارت های ISO ID-1 استفاده می کنند می شود .

- ☐ ابعاد کارت
- ☐ محل قرار گرفتن تراشه (در کارت های تماسی)

- ماده کارشده در کارت ها (برای مثال PVC ، ABS)
- علامت مغناطیسی (اختیاری)
- هولوگرام یا عکس (اختیاری)
- برجسته سازی (اختیاری)
- پارامترهای محیطی

یک کارت هوشمند که مورد تایید ISO 7816 نیز می باشد باید استاندارد لازم برای شرایط فیزیکی (ابعاد کارت) و محل تماس را دشته باشد. محل قرار گرفتن تراشه موضوع بحثی بود که به خاطر بزرگی نوار مغناطیسی مشکلات زیادی به همراه داشت. کارت های فرانسوی اولیه ، ماژول IC را پایین تر از خط تقارن طولی کارت قرار می دادند که در نهایت محل قرار گرفتن امروزی توسط استاندارد تعیین شد .

محل جدید قرار گرفتن تراشه به خاطر خطرات احتمالی موجود در آسیب دیدن تراشه در برابر خم شدگی بسیار ایمن تر بود. استاندارد ISO موجب شد که محل تراشه های فرانسوی نیز تغییر کرده و در محل مصوب قرار بگیرند. ISO 7816 – 2 اجازه می داد که محل کنتاکت ها در هر یک از طرفین کارت تعبیه شود. در سال های اخیر محل قرار گرفتن تراشه از حالت اختیاری خارج شده و فقط در قسمت جلوی کارت (برعکس محل قرار گرفتن نوار مغناطیسی) تراشه ها جاسازی می شوند . انتخاب ماده به کار رفته در کارت، در خواص محیطی محصول تمام شده، اهمیت زیادی دارد. مدت ها است که از PVC به خاطر بالا بودن دقت چاپ در آن، استفاده می شود. این کارت از سه لایه ی شفاف روی هم در جلو و عقب تشکیل شده است در انواع ABS ، کارت بوسیله فرآیند قالب تزریقی بوجود می آید. همچنین پیشنهاد می شود ریز ماژول تراشه در یک مرحله از عملیات قالب گیری جاسازی شود. پایداری حرارتی برای بعضی از کاربردهای بسیار اهمیت دارد و ETSI در این مورد نظارت و توجه خاصی دارد. در چنین تجهیزاتی که با دمای بالا سرو کار دارند ، استفاده از مواد پلی کربنات ضروری است .

۴,۱) خصوصیات MASK ROM (Mask ROM specification)

Mask Rom در برگیرنده سیستم عامل یک کارت هوشمند است. این قسمت تا حد زیادی مرتبط با مدیریت فایل های اطلاعاتی است ولی ممکن است به صورت اختیاری حاوی ویژگی های اضافی مانند الگوریتم پنهانی نیز باشد. از این هنوز در این قسمت استانداردهای مشخص وهماهنگی وجود ندارد.

۵,۱) خصوصیات کاربردی نرم افزار (Application software specification)

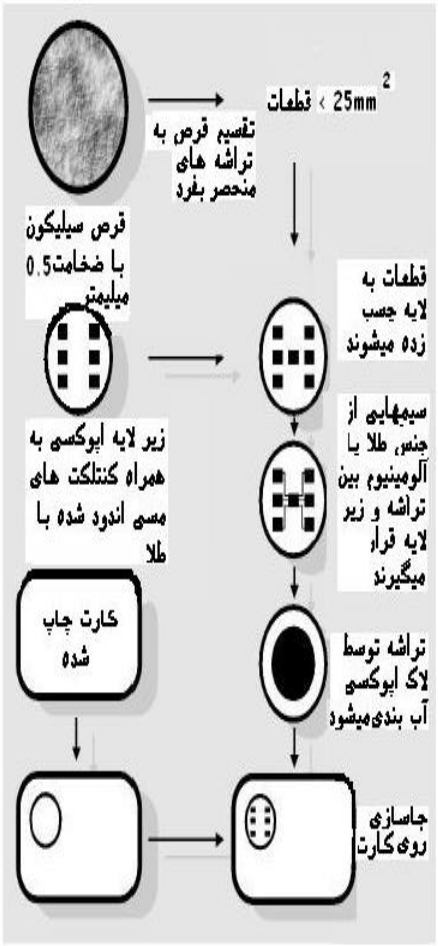
این قسمت از فرآیند ساخت آشکارا بستگی به ویژگی های کاربردی مد نظر دارد. کد کاربرد به عنوان بخشی از کد Mask ROM طراحی می شود. ولی در روش ها وتکنیک های مدرن هدف طراحی یک نرم افزار

کاربردی است ، تا آن چه را که از حافظه غیر فرار PROM دریافت میشود ، انجام دهد. این عمل منجر به این می شود که روش های قابل تغییر بیشتری بعد از اینکه کاربردها بعد از ساخت در کارت بار گذاری شدند ، انجام شود. ساخت یک تراشه با کدهای ROM کاربر، به طور متوسط سه ماه طول می کشد. کدهای کاربردی را می توان در یک دقیقه روی حافظه PROM بدون نیاز به رجوع به سازنده تراشه بارگذاری کرد.

۶,۱) تولید تراشه (Chip fabrication)

ساخت یک کارت هوشمند از چندین فرآیند مختلف تشکیل شده است که در شکل زیر نشان داده شده است.اولین مرحله ساخت لایه ی حاوی تراشه است. این عمل معمولاً COB (chip on board) نامیده می شود و شامل یک تخته اتصال اپوکسی شیشه ای که روی آن تراشه به کانکتور متصل می شود. سه تکنولوژی برای این فرآیند موجود می باشد. ۱- اتصال سیمی[1] ۲- ضربه آرام و ناگهانی به تراشه[2] ۳- اتصال خود کار نواری[3] در هر یک از روش های بالا ، قطعه نازک سیلیکون نیمه هادی ، بوسیله سازنده نیمه هادی تولید می شود و به قطعات کوچک تراشه های اختصاصی بریده می شود. توسط الماس برش هایی صورت می گیرد و با فشار یک غلطک قطعات نازک سیلیکون از نقاطی که توسط الماس مشخص شده اند ترک می خوردند. معمولاً برش ها از روی قطعه نازک سیلیکونی به دلیل استفاده از اره الماسی جدا می شوند. به همین خاطر یک ورقه میلار (پولیستری) به پشت سیلیکون چسبانده می شود تا قطعات جدا شده از غشاء پولیستری جدا نشوند.

[1] - Wire bonding
[2]-Flip chip
[3] - tape automated bonding



شکل ۴. فرآیند ساخت کارت هوشمند

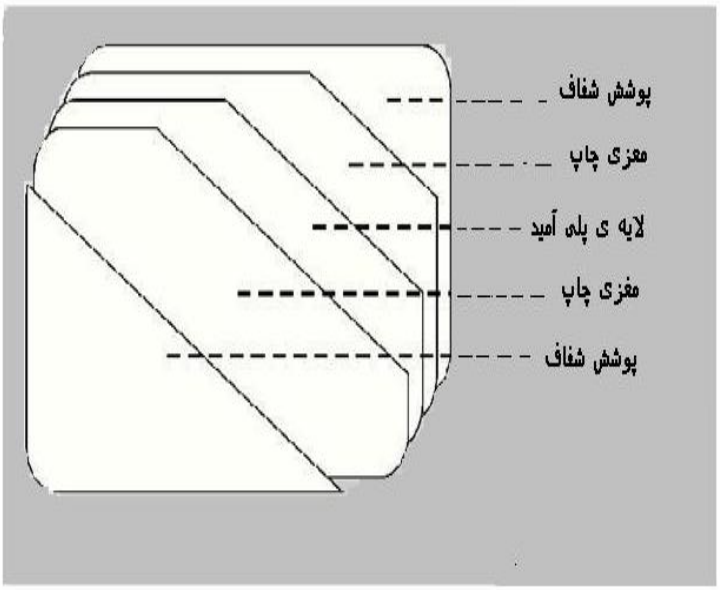
اتصال سیمی رایج ترین تکنیک در ساخت کارت های هوشمند است. یک سیم طلایی یا آلومینیومی 25 uM بوسیله پیوند متراکم حرارتی [1] یافراصوتی [2] به پدِ تراشه متصل می شود. اتصال متراکم حرارتی نیاز به لایه ای دارد که تحمل دمای بین ۱۵۰ تا ۲۰۰ درجه سانتیگراد را داشته باشد. دما در سطح پیوند به ۳۵۰ درجه ی سانتیگراد نیز می رسد.برای رفع این مشکل اغلب از پیوند ترموسونیک استفاده می شود که ترکیبی از دو فرآیند فوق است با این تفاوت که دردمای پایین تری صورت می گیرد .

فرآیند مونتاژ سیلیکون و اتصال سیمی شامل عملیات متعددی است. از این رو مقداری هزینه براست زیرا بطور کلی فقط ۵ یا ۶ سیم که در این روش متصل می شوند، قابل قبول هستند. از این رو در صنعت نیمه هادی معمولاً از دو روش دیگر استفاده می شود(ضربه آرام ناگهانی به تراشه و روش اتصال خود کار نواری). در روش ضربه آرام و ناگهانی به تراشه قطعات بریده شده رو به پایین قرار می گیرند و با لحیم کاری عمل

[1] - thermo Compression
[2] - ultra sonic

اتصال صورت می گیرد. در روش (TAB) قطعات کوچک بوسیله تراکم حرارتی روی کابل هادی که بوسیله یک نوار انعطاف پذیر حمایت می شود ، نصب می شوند. مشابه یک فیلم ۳۵ میلیمتری لایه بدست آمده بصورت سر بسته و محکم با یک ماده بی اثر مانند لاک اپوکسی آب بندی می شود. ریزماژول کامل شده به کارتی که دارای محل مناسب و تعبیه شده است چسب زده می شود .

ساختمان یک کارت بدون تماس قدری متفاوت است زیرا یک کارت از چند لایه تشکیل شده است . IC و اتصال های داخلی آن ، همچنین مدارهای آنتن ها هوایی ، بر روی یک لایه پلی امید[1] انعطاف پذیر قرار داده می شوند .



۷,۱) بارگذاری کاربرد (Application Load)

فرض کنید حافظه مورد نظر روی حافظه PROM یک IC قرار داده شده است. مرحله بعدی کد گذاری حافظه است. این عمل با استفاده از دستورات پایه ای که در سیستم عامل Mask Rom موجود می باشند، انجام می شود. این دستورات امکان خواندن و نوشتن یک حافظه PROM را ایجاد می کنند .

[1] - Polyimide

۸,۱) شخصی کردن کارت (Card Personalization)

یک کارت بوسیله بارگذاری اطلاعات در فایل های موجود در حافظه PROM به یک کاربر اختصاص داده می شود ، همان طوری که کد کاربردی در حافظه بارگذاری می شد .

در این مرحله کلید های امنیتی را می توان روی حافظه PROM بار گذاری کرد .

۹,۱) فعالسازی کاربرد (Application activation)

مرحله پایانی در فرآیند ساخت فراهم آوردن شرایط بهره برداری است. این مرحله شامل نصب پرچم هایی در حافظه PROM می شود. به جز در مواردی که حافظه تحت کنترل مستقیم ابزار باشد و این یک جزء جدایی ناپذیر از فرآیند ایمن سازی کلی است .

۱۰,۱) خصوصیات فیزیکی کارت تماسی

(Physical characteristics of the contact card)

مطالعات گوناگون نشان می دهد که در گذشته، استفاده فراگیر از کارت های هوشمند با توجه به فقدان .استانداردهای لازم امکان پذیر نبود. مشکل اصلی در ایجاد قابلیت همکاری[۱] بود. مشکلات ایجاد قابلیت همکاری با ابعاد فیزیکی و محل قرار گرفتن کنتاکت ها شروع می شد. بخش اول ISO 7816 ویژگی ها و خصوصیات فیزیکی یک کارت IC را معین می کند. این استاندارد مطابق آنچه در ISO 7810 امده است به کارت های شناسایی که دارای نوار مغناطیسی و برجستگی هایی بودند ، اعمال شد. ضمن اینکه همه ما با چگونگی استفاده از حک کننده ها برای بدست آوردن مدل چاپی کاراکترهای حک شده بر روی اوراق معتبر آشنا هستیم، میزان دوام این کاراکترها بر روی یک کارت IC از اهمیت بالایی برخوردار بود. ماژول IC در یک کارت هوشمند مانند تمام ابزار آلات الکترونیکی دیگر است و به طور عادی مجاز به ضربه زدن با چکش یا وسیله سنگین دیگر از یک فاصله معین نمی باشیم. حتی عملیات بر جسته سازی کارت بی تنهایی خود عملیاتی پر دغدغه است و باید برای بدست آوردن استراتژی مناسب ، تمهیدات مناسب اتخاذ شود .

خصوصیات فیزیکی یک کارت IC در ادامه آمده است

ISO 7810 – کارت های شناسایی – خصوصیات فیزیکی – (۱۹۸۵)

[۱] - Interoperability

(ISO 7810 – Identification cards – Physical characteristics (1985))

این استاندارد ویژگی های فیزیکی برای کارت های شناسایی شامل ماده بکار رفته در ساختمان کارت و ویژگی های ابعاد سه سایز مختلف کارت ها (ID -2 , ID-2 , ID – 3) را مشخص می کند .

پارامتر اصلی ISO 7810 ابعاد کارت ID-1 است که اینگونه تعریف می شود:

85.6mm × 53.98mm × 0.76mm

ISO 7811 – کارت های شناسایی - تکنیک های ضبط

(ISO 7811 – Identification cards – recording techniques)

این استاندارد دارای ۵ بخش است و شامل خصوصیات نوار مغناطیسی و برجسته سازی کارت ها می باشد.

بخش اول – برجسته سازی (Embossing)

این بخش از استاندارد ۷۸۱۱ تجهیزات لازم برای حک کردن کاراکترها بر روی کارت شناسایی برای انتقال داده بوسیله دستگاه حک شده یا خواندن ماشینی یا بصری رامشخص می کند.

بخش دوم – نوار مغناطیسی (Magnetic stripe)

این بخش ویژگی های نوار مغناطیسی، تکنیکهای رمزگذاری و تنظیمات کارکتر کد شده را که برای خواندن ماشینی معنی داشته باشد را مشخص می کند.

بخش سوم – محل کارکترهای حک شده بر روی کارت های ID – 1

(Location of embossed characters on ID – 1 cards)

همانطور که درعنوان این بخش آمده است ، محل حک شدن کارکراکترها بر روی کارت ID-1 بوسیله این بخش معین شده است. محل شماره ۱ که می تواند شماره متخص کننده صادره کننده کارت یا نگه دارنده کارت باشد. محل شماره ۲ جهت اطلاعات شناسایی دارنده کارت در نظر گرفته شده است مانند نام و آدرس شخصی دارنده کارت .

بخش ۴- محل قرار گرفتن نوارهای فقط خواندنی مغناطیسی(خطوط ۱و۲)

Location of magnetic read only tracks (lines 1,2)

این استاندارد محل قرار گرفتن ماده مغناطیسی ، خطوط داده رمز گذاری شده و شروع و پایان رمز گزاری را مشخص می کند.

بخش ۵- محل قرار گرفتن نوار مغناطیسی خواندن – نوشتن (خط ۳)

Location of read- write magnetic track (Line 3)

این استاندارد مشابه بخش ۴ است، با این تفاوت که خط ۳ عمل خواندن و همچنین عمل نوشتن را توامان انجام می دهد .

ISO 7812 - کارت های شناسایی – سیستم شماذه گذاری و شیوه ی ثبت نام شناسه ی صادر کننده (۱۹۸۷)

ISO 7812 – Identification cards - Numbering system and registration procedure for issuer identifers– (1987)

این استاندارد از عدد شناسایی و یا PAN (Primary account number) که خود از سه بخش : ۱- شناسایی صادر کننده کارت (IIN) ۲- مشخص کننده حساب فرد ۳- رقم مقابله ای [۱] تشکیل شده است .

ISO 7813 - کارت های شناسایی – کارت های مورد استفاده در تراکنش های مالی (۱۹۸۷)

ISO 7813 – Identification cards – Financial transaction cards (1987)

این استاندارد شرایط لازم برای کارت هایی که در امور داد و ستد مالی مورد استفاده قرار می گیرند را مشخص می کند. این استاندارد خصوصیات فیزیکی ، طرح بندی ها ، تکنیک های ثبت ، سیستم شماره گذاری و روش ثبت کردن را نیز مشخص می کند. این موارد با رجوع به ISO7812 , ISO 7811 , ISO 7810 مشخص می شوند. بطور ویژه استاندارد با جزییات بیشتری ابعاد کارت را همانور که در زیر آمده است مشخص می کند .

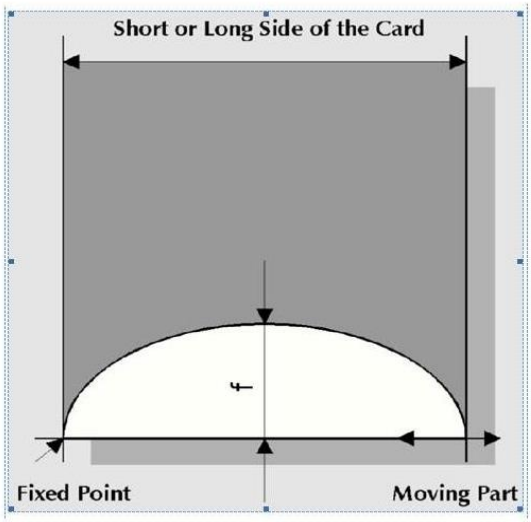
طول 85.47mm-85.72 mm

عرض 53.92mm-54.03 mm

ضخامت 0.76mm ± 0.08 mm

[۱] - check digit

ضخامت کارت هم به نوبه خود برای کارت ها با توجه به مکانیسم ساختمان مکانیکی کانکتورهای مقوله مهمی است.



شکل ۶. آزمایش خمش

این وسیله اغلب از یک کنترل چاپگر قابل حمل تشکیل شده است. در حالیکه فشار و حرکت لازم برای انجام عملیات را ایجاد می کند، کارت را پایین کانکتور قرار می دهد. اختلاف در ضخامت کارت ها و حتی مقدار ناچیزی تاب خوردگی کارت موجب نقص عملیات ارتباطی می شود.

ISO 7816 – طراحی و کاربرد کارت های شناسایی دارای مدار مجتمع با کنتاکت (1987)

ISO 7816 – Design and use of identification cards having integrated circuit with contacts (1987)

این استاندارد و ضمیمه های آن شاید مهمترین ویژگی برای لایه های تحتانی یک IC کارت باشند . به شکل ویژه ای سه بخش اول آن بخوبی بنا نهاده شده است وامکان یک همکاری مشترک فیزیکی و الکتریکی را با معین کردن پروتکل ارتباطی بین کارت IC و وسیله پذیرنده کارت [۱] را ایجاد می کند.

بخش اول – خصوصیات فیزیکی (Physical characteristics)

ابعاد فیزیکی یک کارت IC در ISO 7813 مشخص شده است این نکته حائز اهمیت است که در ضخامت کارت هیچ گونه تمهیداتی برای درج کاراکترهای بر جسته در نظر گرفته نشده است. این بخش همچنین

[۱] - Card acceptor devie

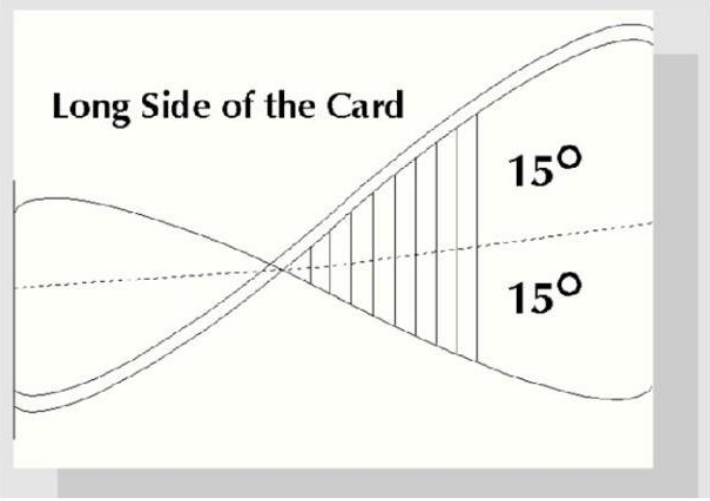
ویژگی های دیگری را که در ساخت یک کارت IC باید در نظر گرفته شود را معین و مشخص می کند. این خصوصیات به بخش های زیر تقسیم می شوند :

- ☐ اشعه ماورابنفش
- ☐ اشعه X
- ☐ تصویر سطح کنتاکت ها
- ☐ توان میکانیکی (برای کارت و کنتاکت ها)
- ☐ مقاومت الکتریکی (برای کنتاکت ها)
- ☐ وجه مشترک الکترومغناطیسی (بین نوار مغناطیسی و مدار مجتمع)
- ☐ میدان الکترومغناطیسی
- ☐ الکتریسیه ساکن
- ☐ اتلاف گرما

این مطلب باید ذکر شود که در این بخش ازاستاندارد ها ، پیشرفت هایی صورت گرفته و در حال حاضر نیز تغییراتی در ISO صورت گرفته است. سه آزمونی که در اکثر مواقع توسط سازنده انجام می گیرد به قرار زیر است

- ☐ A1 خواص خمیدگی
- ☐ A2 خواص پیچ خوردگی
- ☐ A3 الکتریسیته ساکن

یک راه برای مقایسه کارت هایی که توسط شرکت های مختلف ساخته می شوند ، بررسی خواص خمیدگی کارت بوسیله خم کردن کارت حول محورهایی است که در شکل نشان داده شده است .

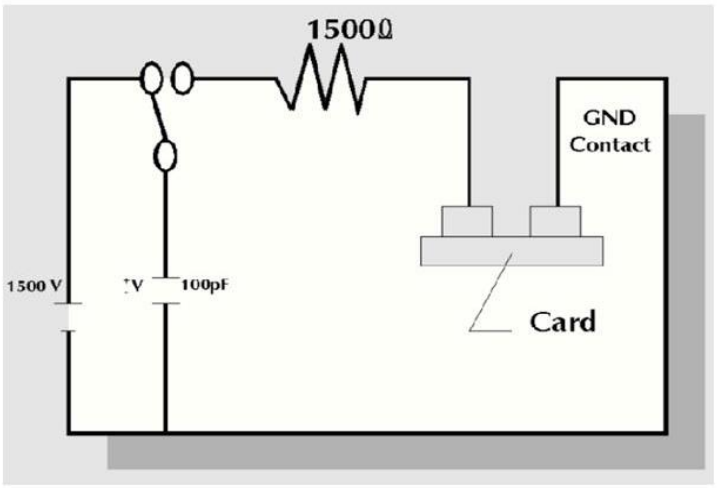


پس از ۳۰ مرتبه خم کردن کارت در دقیقه کارت ۲ سانتیمتر از مرکز خود در راستای محور طولی و ۱ سانتیمتر در راستای محور عرضی خم می شود. این آزمون دوام کارت را در طی ۲۵۰ مرتبه خم شدن کارت درهر یک از ۴ جهت اصلی می آزماید (در مجموع ۱۰۰۰ مرتبه خمیدگی). خواص پیچیدگی کارت با جابه جایی ±۱۵ درجه ای کارت حول محور طولی و به طور پی در پی ۳۰ مرتبه در دقیقه آزموده می شود .

استاندارد موجود در این زمینه ، مقاومت کارت در برابر ۱۰۰۰ مرتبه پیچش ، بدون خواب شدن تراشه یا شکستن آشکار و واضح کارت است .

مقاومت کارت در برابر الکتریسته ساکن بوسیله آزمونی که در شکل نشان داده شده است انجام می شود. ولتاژ آزمون ۱,۵ کیلو ولت معین شده است. کارت باید این ولتاژ را هم در پلاریته مثبت و هم در پلاریته معکوس، در سرتاسر کنتاکت ها تخلیه کند. IC باید در پایان این آزمون قابل استفاده باشد.

یکی از مسائل که مربوط به کارت IC می شود، محدوده ی دمای قابل استفاده این کارت ها است. ISO 7810 معین می کند که یک کارت ID – 1 باید بین دمای 35 درجه تا ۵۰ درجه قابل استفاده باشد. پیش نویس استاندارد CEN که درمورد نیازهای یک کارت IC و ترمینال های مخابراتی است ملزومات سختگیرانه ای را در خود جای داده است؛ برای مثال باید در دمای 35 – درجه تا 65 درجه و گاهاً تا 70 درجه قابل استفاده باشند. در صورتی که این کارت ها شرایط مورد نظر را دارند که حداکثر ۴ ساعت و تا ۱۰۰ مرتبه در پیک های دمایی قرار بگیرد، و بعد از آن قابل استفاده باشند.

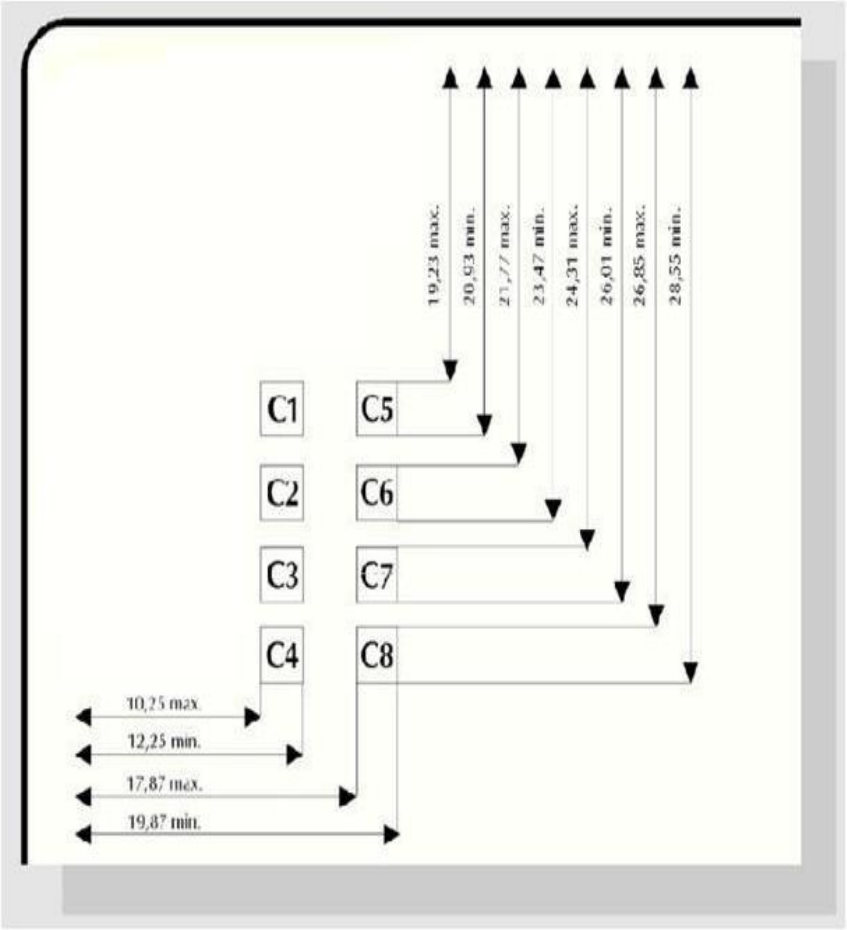


شکل ۸. آزمایش ESD

بخش ۲- ISO 7816 محل قرار گرفتن کنتاکت ها و حداقل اندازه

(ISO 7816 Part 2 – Contact locations and minimum size)

برای رعایت این استاندارد باید کارهای زیادی صورت بگیرد. در استفاده های اولیه از کارت های هوشمند که در فرانسه صورت می گرفت، نوار مغناطیسی Transac مرکزیت بیشتری نسبت به آنچه در نهایت IDO 7811 مشخص کرده داشت. متاسفانه محل اولیه ی تراشه در کارت های هوشمند فرانسوی با مکان در نظر گرفته شده برای نوار مغناطیسی همپوشانی داشت. در نهایت محل کانکتورهای IC مطابق شکل مورد موافقت قرار گرفت (۱۹۹۰).



شکل ۹. محل قرار گرفتن کنتاکت ها

مکان جدید در نظر گرفته شده به محور طولی نزدیک تر بود شاید شما هم در مورد مکان مناسب جهت قرار گرفتن تراشه دچار تردید شده اید تا دربرابر خطرات مکانیکی آسیب کمتری ببینند ولی از توافقات اصولی صورت گرفته نمی تواند چشم پوشی کرد.

مشکلات بعدی هنگام تصمیم گیری در مورد اینکه کدام طرف کارت برای قرار گرفتن کانکتورها مناسب تر است بوجود آمد. برای جلوگیری از تاخیر بیشتر در انتشار استاندارد ها، ISO تصمیم گرفت هر دو طرف کارت را برای تعبیه مکان کانکتورها قابل قبول اعلام کند .

این تصمیم نا متعارف و عجولانه موجب بروز مشکلاتی شد. در نهایت با موافقت های اصولی که صورت گرفت، تصمیم بر این شد که کانکتورها در قسمت جلوی کارت تعبیه شوند. به این منظور پشت کارت ، طرفی از کارت تعریف شد که دارای نوار مغناطیسی است. برجستگی ها نیز در قسمت جلوی کارت (همان طرفی که دارای کانکتور می باشد) مجاز شمرده شد. محل های مربوطه در شکل صفحه ی قبل نشان داده شده است .

۱۱,۱) کارت های هوشمند و تکنولوژی های مرتبط (Smart Cards and related technologies)

در فصل قبل خصوصیات کلی کارت های هوشمند را بررسی کردیم. درادامه به بررسی رایج ترین تکنولوژی های مربط به کارت های هوشمند می پردازیم.

نمای کلی (Overview)

یک کارت هوشمند دارای ابعادی به اندازه کارت های اعتباری است که شامل یک یا چند مدار مجتمع هستند و همچنین ممکن است از یک یا چند نمونه از تکنولوژی های خواندن توسط ماشین زیر برخوردار باشند .

- نوار مغناطیسی
- بار کد (خطی و یا دو بعدی)
- فرستنده فرکانس رادیویی بدون تماس

- اطلاعات بیومتریکی [1]
- سیستم نشانی رمزی
- تعیین هویت تصویری [1]

تراشه مدار مجتمع (ICC) به کار رفته در کارت های هوشمند میتواند مانند یک کامپیوتر یا یک ریز پردازنده عمل کند. اطلاعات در حافظه تراشه ذخیره می شوند و می توان از آنها در دسترسی به کاربردهای پردازشی استفاده کرد. حافظه همچنین حاوی سیستم عامل تراشه [2] ریز پردازنده ، نرم افزار ارتباطی و الگوریتم های پنهانی برای اطلاعات و نرم افزار های کاربردی برای غیر قابل خواندن کردن می باشد. وقتی با ترکیبی از ابزارهای مناسب استفاده شود ، کارت های هوشمند می توانند سطح بالاتری از امنیت و توانایی ضبط و ذخیره و به روز کردن داده ها را فراهم کنند و در صورت استفاده صحیح وبه جا ، کارت هوشمند می تواند میان مراکز و شعب مختلف همکاری همه جانبه ای را بوجود آورند و امکان کاربردهای چند گانه را با استفاده از یک کارت هوشمند ساده ایجاد کنند .

تکنولوژی کارت هوشمند با ارائه امنیت ، مدیریت داده و پشتیبانی مشتریان به صورت حرفه ای تر ، یک سازمان را ایمن تر و کارآمد تر می سازد. این تکنولوژی های بکار رفته در یک کارت است که یک کارت معمولی را تبدیل به کارت هوشمند می کند. تکنولوژی کارت هوشمند از نظر تجاری بسیار اکتیو وموثر است. از این رو سودهای کلانی از طریق تجارت و بازرگانی با تولید انبوه محصولات سخت افزاری و نرم افزاری بدست می آید.

در نهایت کارت هوشمند می تواند منجربه بازنگری و تغییر در فرآیند های ناکارا و تبدیل آن ها به پروژه های با درصد بالایی از احتمال بازگشت سرمایه شود. ترکیب تکنولوژی کارت هوشمند با برنامه ای کاربردی

[1] - biometric information

2- Photo identification

تحت web و استفاده از این کارت ها در تجارت الکترونیک و سایر مشاغلی که با انیترنت سروکار دارند می تواند کیفیت زندگی برای شهروندان و کارمندان را افزایش دهد .

تکنولوژی کارت هوشمند به مشابه یک جعبه ابزار از امکانات تسهیل کننده زیر است:

ابزارهای کنترل دسترسی (Access Control tools)

کارت های هوشمند دارای خصوصیات امنیتی مهمی هستند که این اجازه را به کاربر می دهد که از این کارت ها برای ارائه مجوز لازم جهت دسترسی منطقی و ایمن به ترمینالها و شبکه ها (مانند LAN و اینترنت) و نیز دسترسی فیزیکی به ساختمان ها ، اتاق ها ، محوطه های پارکینگ و سایر تاسیسات استفاده کند .

ابزار پرداخت (Payment tools)

کارتهای هوشمند می توانند ارایه گر خدمات مالی باشند ویا ابزاری برای آگاهی از میزان پرداخت ها و دسترسی به حسابهای مالی وانقال وجه را ممکن سازند.

ابزار مدیریت و ذخیره اطلاعات

(management tools and information storage)

بسته به اندازه ICC ، کارت های هوشمند می توانند اطلاعات را در خود ذخیره و مدیریت کنند؛ برای مثال ، اطلاعات طبی وبهداشتی ذخیره شده روی یک کارت هوشمند می تواند دراختیار یک کارمند بهداشت دارای مجوز در هنگام یک حادثه اورژانسی و یا هنگام یک ویزیت پزشکی عادی مورد استفاده قرار بگیرد. در دسترس بودن اطلاعات روی کارت ، منجر به کاهش زمان لازم برای پیدا کردن نسخه چاپی می شود. اگر وضعیت پزشکی اورژانسی باشد و زندگی فرد در خطر باشد اطلاعات فوراً در دسترس هستند .

دسترسی ایمن پیشرفته (Enhanced secure access)

استفاده از تکنولوژی های پیشرفته و پیچیده ای نظیر بیومتریک ها [۱] و یا PKI [۲] امنیت بیشتری را در سیستم های تشخیص هویت برای دسترسی فیزیکی و منطقی فراهم می کند. PKI از کلیدهای خصوصی وعمومی برای امضاهای دیجیتالی و رمز دار کردن و کشف رمز E-mail استفاده میکند. استفاده از کلید

[۱] - biometrics

[۲] - PKI (Public Key infrastructure)

عمومی فرد امضا کننده ، هنگام بررسی صحت و سقم امضاء دیجیتالی یک فرد مورد استفاده قرار می گیرد . سپس به گیرنده امضا اثبات می شود که بوسیله دارنده حساب امضاء صورت گرفته است. این اطمینان هم برای فرستنده و هم دریافت کننده محرز می شود که اطلاعات عوض نشده است. بیومتریک ها از خصوصیات فیزیکی برای تشخیص هویت فرد استفاده می کنند ، نظیر اثر انگشت ، هندسه کف دست ، اسکن عبیه و تشخیص صدا .

۱۲,۱) انواع مختلف کارتهای دارای تراشه

(Different types of chip cards)

معمولاً واژه های «کارت دارای تراشه» [۱] «کارت مدار مجتمع» [۲] و «کارت هوشمند» [۳] به جای هم به کار می روند. هر کدام از این واژه ها دارای یک معنی و مفهوم خاصی می باشند. کارت ها بوسیله نوع تراشه بکار رفته در آنها و واسطه ای که در ارتباط با ریدر استفاده می کنند، تمیز داده می شوند . سه نوع مختلف تراشه وجود دارد که آنها را می توان در این نوع کارت ها به کار برد: فقط حافظه که شامل حافظه محافظت شده سری و منطق سیم کشی شده و ریز پردازنده است. واژه های «فقط حافظه» ، «منطق سیسم پیچی شده» [۴] و «ریزپردازنده» به امکاناتی که یک تراشه فراهم می کند بر می گردد.

آنچه در ادامه آمده است بحث در مورد انوع مختلف کارتهای دارای تراشه است .

-کارت های تراشه دار مدار مجتمع فقط حافظه

(Memorg only integrated circuit chip cards)

کارت های فقط حافظه آنهایی هستند که دارای نوار مغناطیسی الکترونیکی می باشند وامنیت بیشتری را نسبت به کارت های نوار مغناطیسی معمولی فراهم می کنند دو مزیت این کارت ها نسبت به کارت های نوار مغناطیسی :

ظرفیت داده بالاتر (تا ۱۶ کلیوبایت) و وسایل read / write ارزانتر است.

انواع فقط حافظه کارت های دارای تراشه ، دارای منطق و عملیات محاسباتی نمی باشند. این کارت ها به سادگی داده ها را ذخیره می کنند.یک نوع دیگر، کارت های حافظه درگاه محافظت شده هستند که ویژگی

---

[۱] - chip card

[۲] - Integ rated circuit card

[۳] - smart card

[۴] - Wired logic

های امنیتی بکار رفته درآنها در کارت تراشه ای فقط حافظه موجود نمی باشد. آنها می توانند دارای حافظه سخت افزاری باشند که قابلیت نوشتن مجدد در آن وجود ندارد. انواع اولیه کارت های فقط حافظه read only – بودند و حافظه کمی داشتند (حداکثرتا ۱۶۰ واحد باارزش) و به صورت پیش پرداخت عرضه می شدند و نیز دارای سطح پایینی از امنیت بودند وبعد از مصرف دور انداخته می شدند. این کارت های پیش پرداخت از حافظه read / write استفاده می کنند و برنامه های شمارش دودویی دارند که با کارت امکان حمل و جابجایی بیش از 20 000 مقدار با ارزش را می دهد. همچنین اکثر این کارت ها از برنامه های تعیین صحت و اعتبار بر پایه منطق پیشرفته که در تراشه تعبیه شده است استفاده می کنند. دیگر کارت های فقط حافظه برای اعمالی نظیر بار گذاری مجدد مقادیر ذخیره شده توسعه داده شدند. کارت ها دارای خزانه ای هستند که با استفاده از شماره شناسایی مشخص [۱] و باجه های پرداخت می توان دفعات شارژ خزانه را محدود کرد .

- **کارت های تراشه دار مدار مجتمع منطق سیم کشی شده**

(Wired Logic integrated circuit chip cards)

یک کارت تراشه ای منطق سیم پیچی شده شامل یک ماشین اصلی بر مبنای منطق است که رمز گذاری کردن و تائید دسترسی به حافظه را انجام می دهد. کارت های منطق سیم پیچی شده یک سیستم فایل ثابت را تهیه می کنند که امکان انجام کارهای متعددی را فراهم کنند که به صورت اختیاری می توانند به رمز در آوردن امکان دسترسی به حافظه را دارا باشد. سیستم پرونده ها و دستورات تنظیم شده را فقط با طراحی مجدد منطق IC می توان تغییر داد. کارت های تراشه مجتمع منطق سیم پیچی شده دارای انواع مختلف بدون سیم مانند I-CLASS و MIFARE می باشند .

- **کارت های تراشه دار مدار مجتمع ریزپردازنده ایمن**

(Secure microntroller Integrated circuit chip cards)

کارت های ریزپردازنده دارای یک ریزپردازنده، یک سیستم عامل و حافظه read / write می باشند که بارها می توان آن را به روز کرد. یک کارت تراشه دار ریزپردازنده ایمن از اعمال منطقی و محاسباتی پشتبانی کرده و اطلاعات را در صورت موافقت سیستم عامل ذخیره می کند. کارت دارای ریزپردازنده مانند یک ریز کامپیوتر است که یک فرد می تواند آن را در کیف پول خود حمل کند. تنها چیز که برای شروع به کار نیاز

[۱] - Personal identification number

دارد ، انرژی و تبادل ارتباطی است . IC های ریزپردازنده درانواع تماسی [۱] ، بدون تماس [۲] و دو-رابطی [۳] موجود می باشند.

بر خلاف انواع فقط حافظه ، این IC های ریز پردازنده طوری طراحی می شوند که اهداف امنیتی لازم را برآورده کنند. مانند IC کارت مورداستفاده در وزارت دفاع ایالات متحده آمریکا. این کارت های تراشه دار ریزپردازنده ایمن معمولاً با نام «کارت هوشمند» شناخته می شوند. امروزه فروشندگان، هر دو نوع کارت های فقط حافظه و تراشه دار ریزپردازنده را پیشنهاد می کنند. دراین پروژه ما فقط کارت های تراشه دار ریزپردازنده را توصیه می کنیم. بدلیل سطح پایین امنیت کارت های تراشه دار فقط حافظه و نیز ظرفیت ذخیره محدود برای کاربردهای متعدد یا کارت های چند-منظوره مناسب نیستند.

دو نوع اصلی برای رابطهای کارت های تراشه دار وجوددارد، تماسی و بدون تماس . واژه های «تماسی» و«بدون تماس» چگونگی تأمین توان الکتریکی مورد نیاز ICC را نشان می دهد که بوسیله آن داده از ICC به رابط یک ریدر منتقل می شود. با استفاده از دو تراشه مجزا کارت ها می توانند مجهز به هر دو نوع رابط تماسی و بدون تماس شوند.(اغلب این کارت ها را هایبرید می نامند.) و یا بوسیله یک تراشه دورابطی(به این کارت ها "combi" می گویند)

- **کارت های هوشمند تماسی (contact smart cards)**

یک کارت هوشمند تماسی برای قرار گرفتن در ریدر کارت هوشمند و ارتباط با ریدر نیاز به یک ارتباط مستقیم به یک میکروماژول رسانا که در سطح کارت تعبیه می شود، دارند.

- **کارت های هوشمند بدون تماس (contact less smart cards)**

این کارت ها برای تبادل داده باید در مجاورت ریدر قرار بگیرند.(معمولاً درفاصله ۱۰ سانتیمتر یا ۳/۹۴ اینچی). تبادل داده بدون تماس بوسیله ی امواج RF[۴] صورت می گیرد. آنتن داخلی به کار رفته در کارت و ریدر، ارتباط بین کارت و ریدر را امکان پذیر می کند.

- **کارت های هوشمند هایبرید (Hybrid smart cards)**

---

[۱] - Contact

[۲] - Contactless

[۳] - dual – interfaces

[۴] -Radio frequency

یک کارت هایبرید دارای دو تراشه بر روی یک کارت است که یکی از آنها تماسی ودیگری ارتباط بدون تماس را تامین می کند. دو تراشه موجود در کارت با یکدیگر ارتباطی ندارند.

- **کارت های هوشمند تراشه دار دورابطی**

(Dual-interface chip smart cards)

یک کارت تراشه دار دورابطی از یک تراشه ساده تشکیل شده است که هر دورابط تماسی و بدون تماس را تامین می کند واطلاعات هم از طریق ریدرهای تماسی وهم ریدرهای بدون تماس می توانند در دسترس قرار بگیرند.

۱۳,۱) تراشه ریزپردازنده ایمن

(The secure microcontroller chip)

یک تراشه ریزپردازنده ایمن دارای:

- یک واحد پردازش مرکزی ۸ تا ۳۲ بیتی (cpu)
- حافظه فقط خواندنی (ROM) و حافظه فلش که دارای سیستم عامل تراشه و به طور اختیاری نرم افزار کاربردی می باشد.
- حافظه دستیابی تصادفی (RAM) که به عنوان یک ثبات موقت برای داده به کار می رود.
- انواع دیگر حافظه های غیر فرار که برای ذخیره داده های کاربر مورد استفاده قرار میگیرد(به طور مثال حافظه الکترونیکی پاک شدنی فقط خواندنی (EEPROM)، RAM فروالکتریکی و حافظه فلش).
- خصوصیاتی که اقدامات متقابل در برابر خطرات امنیتی قابل پیش بینی و شناخته شده را انجام می دهند.
- سنسورهای محیطی (برای مثال، ولتاژ ، فرکانس و دما)
- حداقل یک پورت ارتباطی سریال
- تولید کننده شماره های تصادفی
- تایمرها
- موتور(یا موتورهای)رمز نویسی(اختیاری)
- سایر دستگاه های جانبی مرتبط (برای مثال، شتاب دهنده مجموع مقابله ای[۱]، رابطه های سریال[۲] و درگاههای ارتباطی[۳])

آنچه در ادامه آمده است توضیحی درموردانواع حافظه بکار رفته در کارت های هوشمند است.

ROM

[۱] -Checksum accelerator

[۲] -Serial peripheral Interface

[۳] -Communication port

که دارای سیستم عامل تراشه است. سیستم عامل یا مجموعه دستورات، تمام ارتباطات میان تراشه و دنیای خارج را کنترل می کند. سیستم دسترسی به سیستم فایل ها را کنترل می کند. یک ROM ، که در فرایند تولید توسط سازنده نیمه هادی نوشته می شود را دیگر نمی توان تغییر داد.EEPROM یک حافظه غیر فرارّ است (به این معنی که با قطع ناگهانی توان اطلاعات از بین نمی روند) و برای داده های ذخیره شده قابل write/read است. دسترسی به حافظه EEPROM ها بوسیله سیستم عامل تراشه کنترل می شود. EEPROM ها در حاضر می توانند تا ۱۲۸ کیلوبایت حافظه را شامل شوند که قابلیت افزایش تا ۲۵۶ کیلوبایت نیز وجوددارد.

EEPROM ها ممکن است حاوی داده هایی نظیر PIN باشند که دسترسی به آنها فقط توسط سیستم عامل امکان پذیر است. دیگر داده ها، برای مثال سریال کارت در EEPROM هنگامی که کارت ساخته می شود، می تواند قرار گیرد. EEPROM ها معمولاً برای داده های کاربردی وانجام یک عملیات معین به کار می رود. اکثر حافظه های EEPROM برای ذخیره داده های کاربر مانند بیومتریک ها، میزان دارایی، صدور مجوز، اطلاعات دموگرافیک و ضبط ونگهداری تبادلات صورت گرفته به کار می روند.EEPROM ها صدهابار قابل برنامه ریزی مجدد هستند وهم دربلوک وهم در بایت قابلیت پاک شدن را دارند.

FRAM

فروالکتریک RAM که Fe-RAM نیز گفته می شود، دیگر تکنولوژی حافظه غیر فرار است. FRAM داده ها را هزاران مرتبه سریع تر و در ولتاژ بسیار پایین تر، در مقایسه با دیگر ابزارهای حافظه غیرفرار می خواند.FRAM یک حافظه دستیابی تصادفی است که توانایی خواندن ونوشتن سریع دسترسی به دینامیک RAM را ایجاد می کند.

(دینامیک RAM، پرکاربردترین حافظه در کامپیوترهای شخصی است) وهمچنین توانایی حفظ داده ها به هنگام از بین رفتن ناگهانی توان را هم دارا می باشد. (مانند دیگر وسایل حافظه غیر فرار نظیر RAM و حافظه فلش). بخاطر متراکم تر بودن FRAM ها نسبت به DRAM و SRAM (استاتیک RAM که ظرفیت ذخیره بالایی ندارد) احتمال جایگزین کردن این تکنولوژی ها وجود ندارد. با وجود حافظه سریع با یک ولتاژ پایین، انتظار بکار رفتن این تکنولوژی در تلفن ها دستی، توان سنج ها، کارت های هوشمند و سیستم های امنیتی دور از ذهن نیست. FRAM ها به مراتب از حافظه های فلش سریع تر هستند.

انتظار به کاررفتن EEPRAM , SRAM درکاربردهای مختلف در آینده ای نه چندان دور وجود دارد. این حافظه ها پتانسیل لازم برای تبدیل شدن به یک عنصر کلیدی در محصولات بی سیم آینده را نیز دارند.

حافظه فلش (Flash memory):

این حافظه ها که گاها « فلش RAM » نیز نامیده می شوند ، یک نوع حافظه غیر فرار توان ثابت هستند که توانایی پاک شدن و دوباره برنامه نویسی شدن در واحدی از حافظه به نام «بلوک» را دارا می باشند.

حافظه فلش اغلب برای نگهداری کد کنترل مورد استفاده قرار می گیرد، مانند سیستم ورودی / خروجی پایه. در یک کامپیوتر شخصی هنگامی که BIOS نیاز به تغییر (دوباره نوشتن) دارد، حافظه فلش را می توان در بلوک نوشت، از این رو به روز کردن آن به آسانی انجام می شود. محصولات فلش عمومی هستند وکاربرد مورد نیاز را می توان درآخرین مرحله روند تولید درآن ها بارگذاری کرد. این حافظه ها دارای انعطاف پذیری بیشتری هستند و زودتر دراختیار مصرف کننده قرار می گیرند.

با وجود این که روش تولید در انواع حافظه های فلش متفاوت است، این حافظه ها از EEPROM قیمت کمتری دارند. محصولات کنونی را نمی توان بارها برنامه نویسی وپاک کرد و معمولاً امکان برنامه ریزی و پاک کردن در بایت های حافظه وجود ندارد.

به این خاطر به این نوع حافظه «فلش » می گویند که ، تراشه طوری طراحی شده تا بخشی از سلول های حافظه طی یک حرکت ساده پاک شوند ویا به اصطلاح «فلش» شوند. پاک شدگی که به علت تونل Fowler-Nordheim به وجود می آید که شکاف الکترونها در سرتاسر یک ماده دی الکتریک برای خارج کردن بار الکتریکی از گیت شناور مرتبط به هر سلول حافظه می باشد. امروزه یک نوع از حافظه فلش موجود می باشد که در هر سلول حافظه دو بیت را نگه داری می کند. بنابراین با افزایش دوبرابر ظرفیت حافظه در قیمت تغییری صورت نمی گیرد . بعضی از سازندگان تراشه محصولاتی متشکل از ROM ، حافظه فلش و EEPROM تولید می کنند.

RAM

حافظه دستیابی تصادفی که فرارّ است و برای ثبت ذخیره موقت بوسیله ریزپردازنده تراشه مورد استفاده قرار می گیرد. برای مثال از بررسی PIN ، یا خود PIN بوسیله ترمینال فرستاده می شود یا پدِ PIN به صورت موقت در RAM ذخیره می شود .

مثال های زیر درموردکاربر انواع حافظه هایی است که به بحث درمورد آنها پرداختیم.

یک استفاده رایج از کارت دارای تراشه ریزپردازنده، ذخیره سیستم عامل در ROM است. سیستم عامل ومجموعه دستورات به دستوراتی نظیر «خواندن یک رکورد» ، «نوشتن یک رکورد» و «بررسی درستی PIN» که بوسیله ترمینال یا ریدر به کارت ارسال می شود واکنش نشان می دهد. اطالعاتی نظیر میزان سرمایه، شماره سریال کارت، اطلاعات دموگرافیک در EEPROM ذخیره می شوند.CPU تمام اعمال پردازشی را اجرا می کند. هنگام بررسی صحت و سقم PIN ، PIN بطور موقت درRAM ذخیره می شود. با توجه به این که حافظه RAM فرار است، به محض قطع توان مورد نیاز کارت، تمام اطلاعات ذخیره شده در RAM

از بین می روند. هنگام بررسی انواع کارت ها برای انجام یک کار شخصی، میزان حافظه در اجزا مختلف بسیار مهم است. ظرفیت EEPROM یک کارت بسیار حیاتی است، زیرا ظرفیت بیشتر EEPROM فایل های مبادله شده وکاربردهای بیشتری را درخود جای می دهد و همچنین میزان فضای ROM نیز بسیار مهم است، زیرا ظرفیت بیشتر ROM ، سیستم عامل پیچیده تری را درخود جای می دهد که به انجام عملیات سیستمها وکارت های چند کاربردی کمک شایانی می کند.

دربعضی از کارت ها بین ROM , EEPROM ارتباط نزدیکی وجود دارد زیرا بعضی از فروشندگان ترجیح می دهند ، کد مشتری را از سیستم عامل ROM تا EEPROM تعمیم دهند.اگرچه این تکنیک کاربردی بودن کارت را افزایش می دهد ولی از طرف دیگر میزان حجم EEPROM برای ذخیره تبادلات صورت گرفته دیگر کاربردها را نیز کاهش می دهد.

۱۴,۱) وسایل Read/Write کارت های هوشمند

(Smart cards read/write devices)

این دستگاهها ارتباط فیزیکی بین سیستم میزبان و کارت هوشمند را تامین می کنند. سیستم میزبان می تواند یک pc ، یک دستگاه شبکه و یا وسیله کنترل دستیابی مستقل مانند کنترل کننده های گردانی که در ابتدای مراکز مهم نصب می شوند و وظیفه کنترل ورودی را برعهده دارند، باشد. این وسایل توان را دریافت، عمل مقدار دهی را در کارت انجام می دهند وبه عنوان واسط بین میزبان و کارت هوشمند انجام وظیفه می کنند. توان با ایجاد یک ارتباط فیزیکی درکنتاکت های ریزماژول کارت هوشمند یا با القا کردن جریان درطول آنتن های انواع بدون تماس به کارت تحویل داده می شود. قالب کارت های هوشمند بوسیله یک قرارداد معین مشخص شده است که تمام کارت های هوشمند از آن باید تبعیت کنند و ریدرهای سازگار نیز از این قرارداد تبعیت می کنند. بنابراین از لحاظ کاربردی وعملی این مهم باید مورد توجه قرار بگیرد که ریدر انتخاب شده باید از قرارداد مربوط به تراشه ها تبعیت کرده باشد و حتماً قبل از خرید کلی ریدرها ،از قابلیت سازگاری ریدر وکارت اطمینان حاصل کرد.

وسایل read/write مستقل، تمام منطق های مورد نیاز برای مقدار دهی اولیه به یک کارت و عمل کردن به عنوان یک واسطه بین کارت هوشمند ومیزبان را دارا می باشند. برای مثال میزبان ممکن است اطلاعات زیادی را دریافت کند تا از طریق ریدر آن را به کارت منتقل کند. ریدر مجموعه اطلاعات را ارزیابی کرده و گاهاً بسته های اطلاعاتی را به بسته های کوچک تر تقسیم می کند(قبل از ارسال اطلاعات به یک کارت هوشمند). این بدان معناست که میزبان فقط نیاز به ارتباط با ریدر دارد نه کارت هوشمند. سیستم عامل تمام دستوراتی که یک کارت ریزپردازنده درک می کند را معین و مشخص می کند، بنابراین نیازی به استفاده از ریدر نیست.

ریدرهای Transparent به راه اندازهای بیشتری نسبت به انواع مستقل ریدر احتیاج دارند. با این وجود ساختن ریدرهای Transparent ارزان تر وتغییر دادن آنها آسان تر انجام می شود. ریدرهای مستقل گرچه نسبت به انواع Transparent گران تر هستند ولی مجموعه ای از راه اندازهای اصلی دارند که ارتباط بین ریدر ومیزان را مشخص می کند واین یک امتیاز بسیار ارزشمنداست، زیرا طراحی یک معماری سیستم در نهایت به آسانتر شدن اضافه کردن برنامه های کاربردی درآینده و در کل ارتقا عملکرد نرم افزاری را به دنبال دارد.

هزینه های بکارگیری کارت های هوشمند و بعضی از ریدرهای آنها در مقایسه با گسترش یک سیستم قدیمی، برای داشتن یک سیستم کامل بی عیب و نقص بسیار کمتر است. با این وجود وقتی که کارت های هوشمند و ریدرهای آن ها را به صدها یا حتی هزاران کاربر گسترش وتوسعه دهیم، قیمت تجهیزات مبلغ قابل توجهی می شود. برآورد هزینه های سخت افزاری کارت های هوشمند، درانتخاب وسایلی که مطابق با کاربرد عملی و بودجه شما باشد ضروری است. کارت های هوشمند، ریدرها وعملکردهای عملی که شما آن ها را توسعه می دهید و به کار می برید ممکن است در طول روز بارها مورد استفاده قرار گیرند. بنابراین انتخاب سخت افزاری که تا حدامکان قابل اطمینان باشد بسیار مهم است . میزان سطح سرویس دهی حین تامین تجهیزات مورد نیاز اشخاص برآورد می شود.

امروزه انواع مختلفی از وسایل read/write کارت هوشمند و دستگاههای رابطه[۱] در دسترس هستند که نیازهای کاربردهای گوناگون را برآورد می کنند. وسایل read/write کارت هوشمند می توانند یک عملیات ساده را انجام دهند یا توسط وسایل متنوع دیگر کامل شوند، مانند صفحه کلید یک کامپیوتر شخصی . خرید یک ریدر کامل کارت هوشمند با اندازه ای درحدود یک صفحه کلید PC ، سازگاری با سیستم میزبانی که به آن متصل می شود را تضمین می کند و دیگر نیاز به تهیه یک ریدر دارای دو شاخ برای اتصال به پریز با عملکرد ساده درآینده نیست و همچنین نیاز به تهیه هیچ ابزار دیگری برای ایجاد سازگاری با میزبان نیست . یک کاربرد خوب این ریدرها دسترسی منطقی ایمن به سیستم کامپیوتری یا شبکه است. ریدرهای تک کاربردی نیز با اتصال های واسط میزبان متنوعی در دسترس هستند، مانند: صفحه کلید plug-in wedge، درگاه USB ، درگاه سریال و سیم پیچی مستقیم[۲] مانندکنترل فیزیکی دسترسی در کنترل کننده درهای حفاظتی .

ریدرهای کارت هوشمند را به روشهای گوناگون می توان نصب کرد. ریدرهایی که برای کاربردهای عملی نظیرکنترل فیزیکی دسترسی ایمن طراحی می شوند درارتفاع مناسبی از بالای ورودی ها و با سیستم کشی

---

[۱] -inteface device

[۲] -directed-wired

های مخفی از دید به منظور جلوگیری از دستکاری های خرابکارانه قرار می گیرند. وسایل read/write کارت هوشمند را می توان با دیگر وسایل ویژه تلفیق کرد.

از ابزار نوشتن درکارت هوشمند یا رمزگذاری کارت های هوشمند درمرحله شخصی کردن کارت ها استفاده می شود. اکثر سیستم های شخصی کردن کارت ها دارای منطق رمزگذاری کارت های هوشمند هستند که تراشه کارت را قادر می سازد تا اطلاعات شخصی کردن را در کارت جای دهد. بوسیله آن عملیاتی که طی آن داده های بصری ومتنی درکارت قرار می گیرند. این عمل به تضمینی جهت تطابق کاربردهای عملی نرم افزار با داده ها کمک می کند و نیاز به رمزگذاری مجدد درمرحله بعدی نیست.

شکل ۱۱. وسایل READ/WRITE کارت هوشمند

۱۵,۱) رابط های کارت های هوشمند : تماسی وبدون تماس

(Smart cards interfaces: contact and contactless cards)

ارتباط بین کارت های هوشمند با وسایل read/write به شکل های زیر انجام می شود.

تماس الکترونیکی مستقیم

انتقال داده ها به صورت بی سیم توسط فرکانس های رادیویی

تکنیک های تزویج القایی

رابطه های تماسی نیاز به دخول کارت در ریدر دارند تا ریدر بتواند با تراشه یک ارتباط الکتریکی مستقیم داشته باشد.

یک کارت هوشمند بدون تماس از یک تراشه ویک آنتن که بین لایه پلاستیکی احاطه شده ، تشکیل شده است. ارتباطات بواسطه استفاده از تکنولوژی RF بسیار آسان شده است. ارتباط تراشه با آنتن بکار رفته هنگامی برقرار می شود که کارت درمحدوده ۱۰cm (۱/۹۴ اینچی) از ریدرکارت هوشمند قرار می گیرد.

کارت های تماسی به طور کلی برای کاربردهای گوناگون مورد استفاده قرار می گیرند من جمله تبادلات مالی وکنترل منطقی دسترسی. تراشه های بدون تماس به عنوان مثال در کاربردهایی مورد استفاده قرار می گیرند که نیاز به سرعت بیشتر وعملکرد ساده تر وجود دارد.

یک کارت تماسی، بدون تماس ویا چند-رابطی، عملیات متعددی را می توانند انجام دهد که مزیت ها ی زیادی هم برای تشکیلات صادر کننده کارت وهم دارنده کارت به همراه دارد. تشکیلات صادر کننده کارت چندین تکنولوژی را با هم ترکیب کرده و برای وضعیت های متفاوت ، تدابیر امنیتی متفاوتی را پشتیبانی می کند. اعمالی نظیر دسترسی منطقی به شبکه های کامپیوتری ، پرداخت های الکترونیکی، خرید وفروش بلیت های الکترونیکی را می توان با دسترسی فیزیکی در یک کارت شناسایی چند تکنولوژی وچند کاربردی ترکیب کرد. صادر کننده همچنین می تواند ثبت وذخیره امتیازات و به روز کردن آن ها را از یک مکان مرکزی ساده انجام دهد. برای دسترسی فیزیکی، سازمان با حفظ اجزاء مکانیکی و ریدر در مقابل خطرات ناشی ازاستفاده نا صحیح و خرابکارانه هزینه کمتری بابت تعمیر و نگهداری سیستم پرداخت می کند.

سه تکنولوژی عمده در کارت های بدون تماس جهت کاربردهای کنترل فیزیکی دسترسی مطرح شده است.

تکنولوژی های ISO/IEC 1443 ، ISO/IEC 15693 و 125 KHz

- ISO/IEC 15693 و ISO/IEC 14443

تکنولوژی کارت های هوشمند بی تماس 13.56 MHz بر مبنای استانداردهای ISO/IEC 14443 یا ISO/IEC 15693 بنا نهاده شده است. کارت هایی که با این استانداردها تطابق دارند وسایل read/write باهوشی هستند که قابلیت ذخیره انواع مختلف داده وعمل کردن در رنج های متفاوت را دارا می باشند. کارت های هومشندی که از استانداردها تبعیت می کنند، به درستی هویت شخص را می توانند بررسی کنند و میزان

دسترسی مجاز او را تعیین نمایند و به دارنده کارت اجازه بهره مند شدن از تمامی داده های ذخیهر شده در کارت را می دهند. این کارت ها می توانند حاوی امکانات اضافی صحت وسقم هویت دارنده کارت نظیر مشخصات ظاهری ویا PIN باشند و همچنین ممکن است که از تراشه کارت هوشمند تماسی برای رفع نیازهای کاربردهایی که به تکنولوژی های متفاوت دیگر پاسخ بهتری می دهند استفاده شود.

- ISO/IEC 14443:

در جهت سازگاری بیشتر با استاندارد ISO/IEC 7816 که مربوط به استانداردهای کارت هوشمند تماسی بود، دچار تغییرات زیادی گردید. کارت های هوشمند مطابق با استاندارد ISO/IEC 1443 (بخش های ۱ تا۴) از یک سیستم کامل جهت انتقال دستورات و داده ها بین کارت و ریدر بهره می برند. مادامیکه از رابط الکتریکی بدون تماس به جای رابطه الکتریکی تماسی استفاده شود، نحوه تبادل اطلاعات بین کارت و ریدر مشابه است. ISO /IEC 14443 بگونه ای طراحی شده است تا عملکرد ضعیفی درمحدوده خارج از ۱۰سانتیمتر معین شده، داشته باشد. برای ایجاد ارتباط با کارت از یک فاصله به اندازه کافی دور نیاز به تحریک کارت توسط یک آنتن بی نهایت بزرگ است ، زیرا IC از آن فاصله قابل تشخیص نمی باشد. ذکر این نکته نیز ضروری است که اگر IC دارای سیستم بررسی صحت و سقم هویت فرد باشد و نیز رمزدار شده باشد به محتویات کارت درهر موردی نمی توان دست پیدا کرد.

- ISO/IEC 15693:

برای توسعه اعمال منطقی، برچسب گذاری و کاربردهای کشاورزی شکل رفت و بطور کلی درمواردی که نیاز به ارسال حجم کوچکی داده درفواصل طولانی وجود داشت. اگر چه این استاندارد هم مثل ISO/IEC14443 دارای ۴ بخش است ، قرارداد مربوط به لایه های درجهت سازگاری با ISO/IEC7816 طراحی نشده است.

کارت هایی که از این استانداردها پیروی می کنند از نظر تجارتی توسعه پیدا کردند و جایگاه ثابتی در بازار دادوستد دارند.فروشندگان قادر به تهیه وسایل استاندارد لازم برای تکمیل یک سیستم دسترسی فیزیکی بدون تماس هستند تاخریداران تکنولوژی وتجهیزات را با قیمت های رقابتی خریداری نمایند.

- 125KHz:

توسط اکثر سیستم های کنترل دسترسی RFID امروزی مورداستفاده قرار می گیرد. این سیستم ها بیشتر بر مبنای استانداردهای صنعتی وغیر رسمی هستند تا استاندارد بین المللی.

شکل زیر ارائه گر مقایسه عملکرد انواع تکنولوژی های بدون تماس است و همچنین مثال هایی از خصوصیات هر یک از آن را نشان می دهد(مانند اندازه حافظه و روشهای رمزگذاری کردن).

مقایسه تکنولوژی های بدون تماس			
انواع	14443	15693	125 kHz
استانداردها	ISO/IEC 14443 ISO/IEC 7810	ISO/IEC 15693 ISO/IEC 7810	فاقد استاندارد رسمی
فرکانس	13.56 MHz	13.56 MHz	125 KHz
محدوده خواندن	تا 10 سانتیمتر	تا 1 متر	تا 1 متر
نوع تراشه	حافظه منطق سیم کشی شده ریزپردازنده ایمن	حافظه منطق سیم کشی شده	حافظه منطقی سیم کشی شده
عملیات رمز دار کردن و تعیین اعتبار وصحت	رمزدار کردن MIFARE DES/3DES, AES, RSA	کاربرداز-معین DES/3DES	کاربرداز-معین
محدوده ظرفیت انباره	64 TO 72K Bytes	256 TO 2K Bytes	8 TO 256 Bytes
توانایی READ/WRITE	READ/WRITE	READ/WRITE	فقط READ
میزان انتقال داده Kbytes/SEC	تا 106 (ISO) تا 868 (در عمل)	تا 26.6	تا 4
Anti-collision	دارد	دارد	نوری
قابلیت ارتباط با کارت هایبرید	بلی	بلی	بلی
پشتیبانی از رابطهای تماسی	بلی	بلی	بلی

شکل ۱۲. مقایسه ی تکنولوژی های بدون تماس

کاربردهای دسترسی فیزیکی (Physical access application)

وسایل بدون تماس توسعه پیدا کرده و تکنولوژی ها استاندارد شدند. این پیشرفت ها به منظور داشتن یک کاربرد دسترسی فیزیکی سریع و قابل اعتماد در تبادل داده صورت گرفت. کاربردهای دسترسی فیزیکی معمولاً نیاز به ارائه مجوز مجاز توسط کاربر برای ارائه در ورودی محافظت شده ی محل های بازرسی دارند. درصورت مجاز بودن، به کاربر اجازه دسترسی به مکان مورد نظر داده می شود. برای کاربردهای دسترسی فیزیکی ، تکنولوژی بودن تماس، خروجی سریع وموثقی را ارائه می کند. درصورت استفاده از دیگر وسایل بررسی هویت نظیر تشخیص اثر انگشت مزیت های خروجی تکنولوژی بدون تماس کم شده ولی درعوض امنیت و تشخیص هویت افراد در سطح بالاتری انجام می شود.

درمکان هایی شرایط محیطی مناسب وجود ندارد. نظیر این که ریدر در معرض بارش های سنگین قرار بگیرد یا آلاینده ها درمحیط وجود داشته باشند. استفاده از تکنولوژی بدون تماس مزایای قابل توجهی نسبت به استفاده از تکنولوژی تماسی دارد. همچنین ریدرهای بدون تماس دربرابر تخریب ها و دستکاری های غیرمجاز مقاومت وپایداری بیشتری دارند وهمچنین فقدان بخش های مکانیکی محرک به طرز محسوسی هزینه های تعمیر و نگه داری آنها را کاهش می دهد.

کاربردهای دسترسی منطقی (Logical access application)

در حال حاضر تنها تکنولوژی تماسی روش های مفیدی (از لحاظ مالی) درانتقال مقدار قابل توجهی از داده ها بین یک کارت، یک ریدر و سیستم میزبان فراهم می کنند. بعلاوه تراشه های تماسی دارای ریزپردازنده هستند در حالی که در تراشه های بدون تماس ریزپردازنده به صورت اختیاری می تواند وجود داشته باشد. به این دلایل کارت های هوشمند تماسی پیشنهادهای مناسبی برای جلب توجه کاربران دستگاههای امنیتی یک شبکه هستند.

برای جلب توجه کاربران برای داشتن یک مجوز ID ساده، استفاده از یک کارت بدون تماس هم برای دسترسی فیزیکی و هم منطقی جالب وجذاب است. با توجه به نیازهای یک سیستم ، امروزه می توان از یک کارت هوشمند بدون تماس، جهت تامین نیازهای امنیتی دسترسی منطقی استفاده کرد.

۱۶,۱) تکنولوژی های چندگانه و کارت های چندرابطی

(Multiple technologies and multiple interfaces cards)

امروزه سازمان ها هنگام انتخاب تکنولوژی کارت های هوشمند مناسب، با گزینه های زیادی روبه رو هستند که شامل تکنولوژی های چندگانه وکارت های چندرابطی می شود. یک چالش رایج برای مدیران پروژه در توسعه یک سیستم کسب اطمینان خاطر از قابلیت همکاری سیستم جدید با دیگر سیستم های قبلی باقیمانده است؛ برای مثال کاربر از کارت های هوشمند جدید برای ایجاد ارتباط مستقیم با سیستم کنترل

فیزیکی دسترسی موجود که از تکنولوژی قدیمی تری بهره می برد می خواهد استفاده کند. برای ایجاد تطابق،کارت جدید ممکن است دارای تکنولوژی تراشه هوشمند تماسی یا بدون تماس، نوار مغناطیسی ، بارکد، نوار نوری و یا آنتن مجاور ۱۲۵ کیلوهرتزی باشد. یک کارت که دارای چندین نوع وسیله read/write می باشد به طور کلی «کارت چندتکنولوژی»[۱] نامیده می شود.

کارت های چند تکنولوژی همچنین قادر به ترکیب استاندارد ISO/IEC تکنولوژی های کارت هوشمند بدون تماس با تکنولوژی ۱۲۵ کیلوهرتزی هستند. این ترتیب کارت را قادر می سازد تا با سیستم های کنترل فیزیکی دسترسی قبلی بخوبی سیستم های تحت ISO/IEC عمل کنند. تهیه کردن امکانات چند read/write روی یک کارت اغلب به تهیه ابزارهای مورد نیاز برای تغییر تکنولوژی قدیمی به جدید کمک می کند. بعلاوه ریدرهایی در دسترس هستند که می توانند از سیستم های کارت قبلی پشتیبانی کرده و در تغییر تکنولوژی به کار رفته در کارت به یک تکنولوژی جدیدتر مورد استفاده قرار گیرند.

کلیه تکنولوژی های بکار رفته در یک کارت یک هدف مشخص را دنبال می کنند. با این وجود به همان اندازه هم می توانند سبب بروز یک مشکل پنهانی شوند. با در نظر گرفتن کارت ID هوشمند چندتکنولوژی بیاد داشته باشید که ترکیب شمار محدودی از تکنولوژی های ID سازگار ممکن است به راه حلی سودمند و مفید ختم شود، گرچه مابقی ترکیب ها گاهاً غیرممکن و دراجرا غیر کاربردی وغیر عملی است. از نظر تکنیکی ترکیب چند تکنولوژی متفاوت روی یک کارت امکان پذیر است ولی درکل باید نتیجه نهایی کار مورد توجه قرار بگیرد. کارت های چندتکنولوژی دارای محدودیت های زیر هستند:

- تکنولوژی های بدون تماس چندگانه که در یک فرکانس کار می کنند
- ضخامت کارت
- محل برجستگی ها
- شماره چاپ
- قیمت کارت

ترکیب شمار محدودی از تکنولوژی های ID سازگار روی یک کارت درمقایسه با ترکیب چندین تکنولوژی روی یک کارت، ساده تر و مقرون به صرفه تر است. گرچه کارت های چندتکنولوژی راه حل های مناسبی جهت تطبیق با سیستم های کنترل منطقی ایجاد می کنند بااین وجود ارگان ها باید توجه بیشتری به پیچیده بودن این تکنولوژی ها و نیز هزینه نگهداری و تعمیر آنها داشته باشند.

امروزهاز کارت های هوشمند چندرابطی به طرق گوناگونی استفاده می شود. کارت های هوشمند می توانند از تراشه های دورابطی به عنوان یک کارت ساده برای کاربردهای تماسی و بدون تماس بهره می برند. وقتی

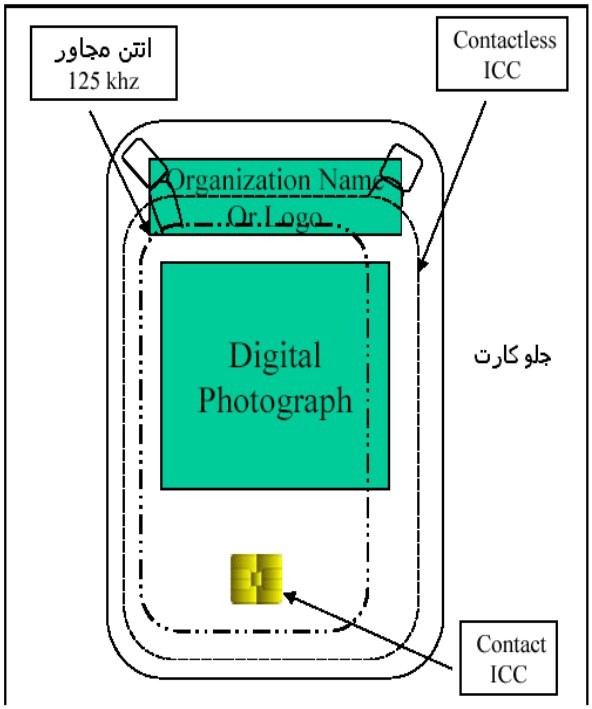
[۱] -multiple technology cards

که از یک تراشه دورابطی استفاده می شود تکنولوژی های تماسی و بدون تماس روی یک ICC ساده برروی کارت هوشمند ترکیب می شوند. این ترکیب تراشه هوشمند را قادر می سازد تا با هردوی ریدرهای تماسی و بدون تماس سازگاری داشته باشد. کاربر ممکن است این ترکیب را هنگامی که ریدر تماسی و بدون تماس موجود می باشند در یک قالب ساده مورد استفاده قرار دهد.

امروزه دربازارکارت های هایبرید نیز موجود می باشند. این کارت ها معمولاً دارای دو ICC هستند. یک تراشه تماسی و یک تراشه بدون تماس. کاربر هنگامی که می خواهد هر یک از تراشه ها کاربردهای متفاوتی داشته باشند یا سازگاری پردازشی بیشتر وجود داشته باشد این ترکیب را انتخاب می کند. این محصولات به شرکت ها این اجازه را می دهد که با استفاده از یک سیستم ساده هم کاربردهای کنترل فیزیکی دسترسی بدون تماس و هم کاربردهایی که نیاز به رابطهای تماسی دارند مانند دسترسی منطقی به کامپیوترها و شبکه ها را توامان داشته باشند.

استفاده از تکنولوژی های مختلف مزیت های امنیتی زیادی به همراه سودهای مالی هنگفت به همراه دارد. ارگان ها می توانند با پیوند دسترسی فیزیکی و دسترسی منطقی درجهت افزایش امنیت گام بردارند. برای مثال، نیاز به استفاده از کارت ID هوشمند هنگام خروج از یک ساختمان ، لیست افراد حاضر در ساختمان هنگام رخ دادن حوادث طبیعی در دسترس است. از این رو روند امداد رسانی به طرز چشمگیری افزایش پیدا می کند. استفاده از تکنولوژی های چندگانه برروی یک کارت ID ساده به طور کلی هزینه های اجرائی و صدور کارت را کاهش می دهد.

شکل زیر نمونه ای از قسمت جلوی کارت هوشمندی را که دارای چندین تکنولوژی است را نشان می دهد.



این کارت دارای تراشه مدار مجتمع تماسی ، تراشه بدون تماس و آنتن مجاور ۱۲۵ کیلوهرتزی است.

۱۷,۱) کارت های چندکاربردی (Multi application cards)

تکنولوژی کارت هوشمند امکان قرار دادن کاربرهای متعدد را روی یک کارت فراهم می کند.

از کارت چندکاربردی در کاربردهای زیر استفاده می شود.

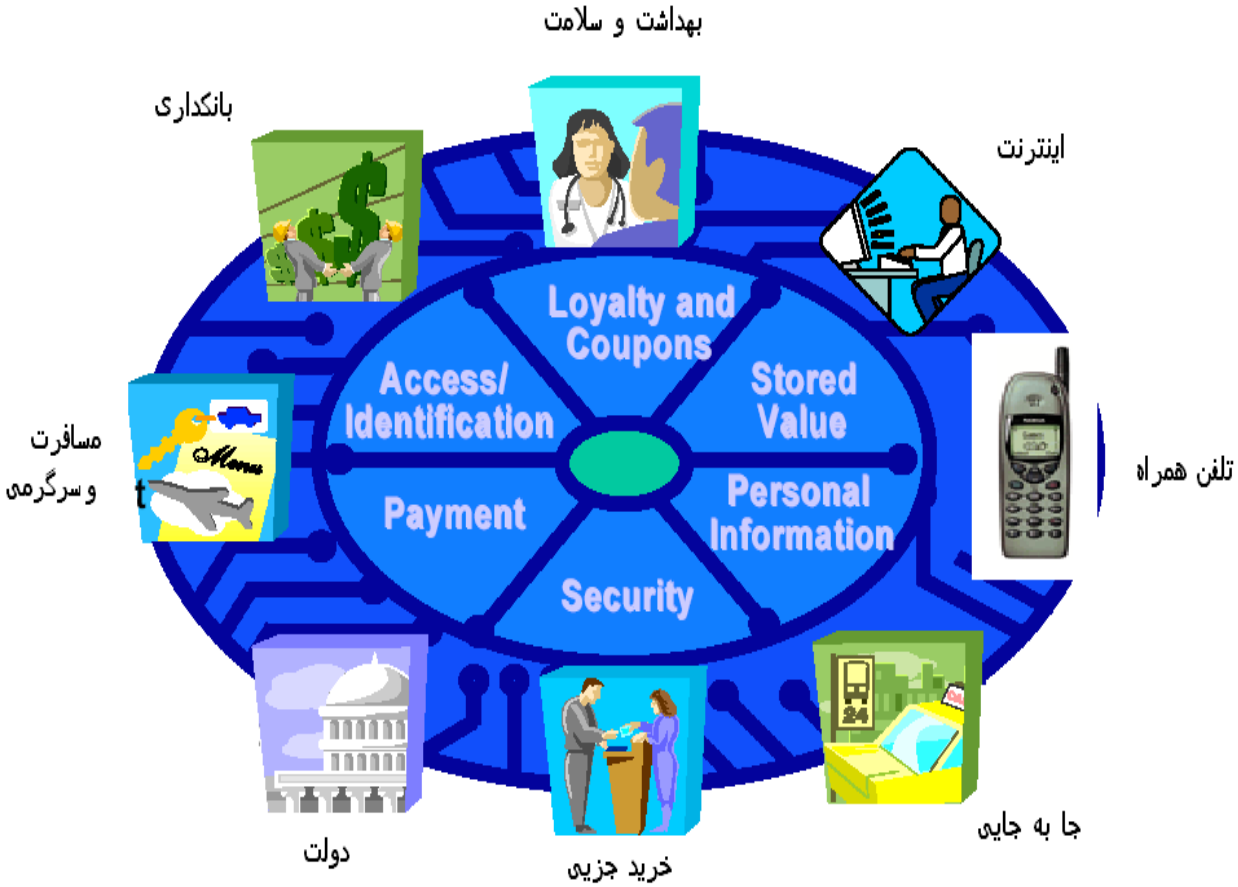
- امضاهای الکترونیکی در E-mail ، رمزدار کردن E-mail
- پرداخت های مالی توسط کیف پول الکترونیکی
- اجازه ورود به مکان های حفاظت شده
- دسترسی منطقی به سیستم های کامپیوتری
- استفاده از داده های ذخیره شده برای دسترسی به اطلاعات پزشکی

کارت های هوشمند تماسی و کارت های هوشمند بدون تماس می توانند از کاربردهای چندگانه پشتیبانی می کنند.

هنگام استفاده از کارت های چندکاربردی، هر کاربرد بوسیله یک تیم مجزا در یک ارگان مدیریت می شود. اگر نیاز به هماهنگی سازمانی پیچیده تری باشد، استفاده از کاربردهای چندگانه تأییدی برای پذیرش کارتهای هوشمند در زمینه های تجاری مختلف است.

یک نمونه از کارت های چندکاربردی کارت های دانشجویی است، که در پردیس دانشگاه مورداستفاده قرار می گیرند. یک دانشجو با استفاده از این کارت ها به امکانات دانشگاه دسترسی پیدا می کند. درکتابخانه دانشگاه از کتاب ها و مراجع آموزشی استفاده می کند. در سلف سرویس غذا سفارش می دهد. کالای مورد نیاز خود را از فروشگاههای دانشگاه خریداری می کند. به علاوه با استفاده از این کارت ها می توان از سیستم های کامپیوتری دانشگاه، شبکه، اینترانت واینترنت درصورتی که این کاربردها درطراحی اولیه کارت مد نظر قرار گرفته شده باشند، استفاده کرد.

تصویر زیر، امکانات بالقوه کارت های چند کاربردی را نشان می دهد.



کارت سیستم باز وجود دارد. در این محیط ،همگرایی تجهیزات دارای استانداردهای بین المللی، برای

افزایش قابلیت همکاری حیاتی و ضروری است، جایی که دولت، صنعت و جامعه می توانند مجوزهای یکدیگر را پذیرفته و سودها و مزیت های فراوانی نصیب طرفین شود.

صادرکنندگان کارت، هنگام طراحی کارت هوشمند چندکاربردی با انتخاب های گوناگونی رو به رو هستند. تفاوت می تواند درآرم شرکت ها، عکس های دیجیتالی و اطلاعات چاپ شده روی کارت باشد. سایر تفاوت ها در تکنولوژی های بکار رفته مانند تراشه های تماسی و بدون تماس ،بارکدها ونوار مغناطیسی است.

هنگام طراحی یک کارت IP ، باید در تکنولوژی بکار رفته در کارت نیازهای حال و آینده پیش بینی شده باشد. تلاش برای پیاده سازی این مهم نیاز به ارتباط و همکاری نزدیک حوزه های IT، امنیت و منابع انسانی با دیگر حوزه ها دارد. استفاده از زیربنای موجود زمانی ممکن است که تلاش های کاربردی به سودهای مالی و صرفه جویی در وقت منجر شود. بخشی از چالش در توسعه سیستم کارت هوشمند چندکاربردی و چندعملیاتی، توسعه زیربنای پشتیبان کارت است. به علاوه سازمان ها باید به نیازهای صدور و تجهیزات مدیریت کارت توجه کافی داشته باشند ، نظیر صدور کلی به جای صدور موردی، تجدید صدور، محل فردنگهدارنده کارت و اطلاعات مدیریت کارت، مدیریت اعتبارنامه ها و کارتهای گم شده یا دزدیده شده.

برای مثال دارنده یک ID کارت دانشگاهی در مثال قبلی ممکن است خواستار صدور مجدد کارت برای استفاده از امکانات بیشتری که برای سایر هم مقطعی های وی فراهم نیست، باشد، در این صورت صدور مجدد کارت دانشگاهی در صورتی که کارت برای کاربردهای متعددی طراحی شده باشد، بسیار پیچیده می شود. قبل از صدور یک کارت دانشگاهی جدید، ابتدا باید هویت فرد و شایستگی فرد برای داشتن امکانات اضافی احراز شود. میزان اندوخته های باقیمانده قبلی و همچنین اطلاعات فردی باید به کارت جدید منتقل شود.

انتخاب سیستم عامل مناسب در موفقیت کارت بسیار حیاتی و ضروری است. انتخاب سیستم عامل مناسب قابلیت کارت را در پیکربندی مجدد بعد از صدور را افزایش می دهد. در بسیاری از موارد، شرکت سازنده در ابتدا یک کارت با یک کاربرد ساده ارائه می کند. هنگامیکه مقبولیت کارت افزایش پیدا کرد و فرصتهای فروش و بازارهای جدید بوجودآمد، سازنده قابلیت کارت را با اضافه کردن کاربردهای جدید افزایش می دهد. یک سیستم عامل باز، به هر کارتی اجازه افزایش امکانات بیشتر را هنگام مقبولیت کارت در بازار و نزد مصرف کنندگان می دهد. دو سیستم عاملی که دارای استانداردهای بیشتری در صنعت کارت های هوشمند هستند، کارت های جاوا و کارت های MULTOS هستند. معیارهای Global Platform استانداردهایی را جهت زیربنای کارت های هوشمند باز در نظر گرفته است که سرویس دهنده را قادر می سازد تا با گسترش و به کاربردن صنایع مختلف کاربردهای چندگانه برای مشتریان خود را بوسیله ابزارآلات متنوع مدیریت کنند. توانایی یک کارت چندکاربردی به توانایی آن در قابلیت ذخیره و پردازش داده بر می

گردد. بنابراین دسترسی ایمن به کاربردهای چندگانه بوسیله یک کارت ساده درمحیط سیستم های باز و بسته بدست می آید. کاربردهایی معین شده که درآنها باید به یک مجموعه معمولی از داده های به اشتراک گذاشته و سرویس هایی که نیاز به کاربردهای بی همتای مستقل دارند دسترسی پیدا کرد. به علاوه هر کاربرد باید از منطق و داده های خود در برابر دیگر کاربردها و کاربران محافظت کند. این عمل بوسیله تکنولوژی چندگانه و تبعیت از استانداردهای رایج نظیر ISO , EMV , GSC-IS2-1 , Global Platform IEC14443 و غیره بدست می آید. در بیشتر موارد توافق بر سر یک مدل داده معمولی که ویژگی های فرض مورد نیاز را برآورده ساخته و یک طراح تکنولوژیکی که قابلیت تطابق پذیری و تغییر را داشته باشد و همچنین صرفه جویی مالی هنگام تولید انبوه و قابلیت همکاری مشترک مناسب برای کارت های چندکاربردی به وجود آورد، بدست می آید.

فصل دوم : اجزا و مولفه های یک سیستم کارتی هوشمند

(Component of a smart card system)

پیکربندی پلت فرم کارت های هوشمند اساساً از یک پروژه تا پروژه دیگر با توجه به اهداف مدیرتی کارت، شخصی کردن کارت، روش های صدور کارت، امکانات و کاربردهای کارت و محیط تخصصی که توسط پروژه انتخاب می شود، متفاوت است. با این وجود مولفه های کلی زیر معمولاً در پلت فرم کارت شناسایی هوشمند یک کارمند که دارای PKI است، موجود می باشند:

Cards (۱,۲

کارت های هوشمند دارای یک ICC می باشند که توان محاسباتی مورد نیاز را تامین می کند. کارت های هوشمند توانایی به کاربردن تکنولوژی های متعددی جهت هویت دادن به کارت نظیر PKI و روش های بیومتریکی [۱] را دارا می باشند. کارت های هوشمند به طور کلی هم برای دسترسی فیزیکی وهم برای دسترسی منطقی مورد استفاده قرار می گیرد و در هر دو نوع تماسی و بدون تماس دردسترس هستند.

۲,۲) سیستم مدیریت کارت مرکزی :

(Central card management system)

سیستم مدیریت کارت مرکزی همانند هسته سیستم کارت هوشمند عمل می کند. این سیستم نیاز به ایجاد اتصال و ارتباط با دیگر اجزا سیستم دارد و درخود پایگاه داده دارنده کارت را جای داده است که با ایجاد امکان ثبت و ضبط و بازیابی، نگهداری و مدیریت داده ها به مدیریت چرخه دوام [۲] کارت های هوشمند کمک شایانی می کند. LCM شامل مراحل پیش صدور، صدور، وضعیت، جایگزینی، امکانات وارد کردن اطلاعات جدید و حسابرسی کارت های هوشمند برای هر شرکت می باشد.

۳,۲) نرم افزار و تجهیزات کارت های هوشمند:

(Smart cards software and equipment)

این نرم افزارها و تجهیزات شامل کامپیوترها، دستگاههای جانبی ونرم افزار مورد نیاز برای تثبیت دارد که جهت عضویت دادن به دارنده کارت شخصی کردن کارت، صدورکارت، امکانات وارد کردن اطلاعات جدید نظیر PIN و به روز کردن اسناد موجود در کارت می باشد.

---

[۱] -Biometrics

[۲] -Life cycle management(LCM)

تجهیزات صدور کارت معمولاً شامل:

- **مرکز ثبت نام (Enrollment workstation)**

مرکز ثبت نام به عنوان مرکزی برای ثبت اطلاعات افراد و تثبیت این اطلاعات در سیستم مدیریت مرکزی کارت و در واقع به منظور شخصی کردن امکانات و تجهیزات متعلق به یک فرد و در نهایت آماده شدن کارت ها برای صدور درنظر گرفته می شود.

با توجه به صلاحدید آژانس ها، متعلقات مرکز ثبت نام شامل یک دوربین دیجیتالی برای ثبت عکس دارنده کارت، وسایل ثبت امضای دیجیتال شده، یک وسیله برای ثبت بیومتریک ها که معمولاً دراین مراکز از وسایل ثبت اثر انگشت استفاده می شود و یک صفحه کلید برای ایجاد PIN توسط کاربر می باشد. در بعضی از کاربردها، داده های بیومتریکی و یا کلیدهای عمومی ثبت شده در مرکز ثبت نام را می توان مستقیماً به قسمت بررسی مجوز صلاحیت درمرکز، به عنوان بخشی از پروسه درخواست مجوز انتقال داد.

- **مرکز تولید کلید (key generation workstation)**

اگر چه جفت کلیدها عموماً بوسیله پردازشگر مرکزی در کارت تولید می شوند، بعضی از آژانس ها ممکن است از یک مرکز مجزا برای تولید کلیدها استفاده کنند(استفاده از نرم افزارهای تولید کلید به جای استفاده از کلید تولیدی دارای علامت مشخصه). پس از تولید یک کلید در مرحله صدور و شخصی کردن کارت، کلید با امنیت بسیار بالایی در کارت بارگذاری می شود. روش دیگر، روش مدیریت کلیداست.

- **سیستم شخصی کردن کارت (Card personalization system)**

از سیستم شخصی کردن کارت به منظور شخصی کردن کارت توسط داده، عکس، جفت کلیدها و صفات مشخصه فرد استفاده می شود. درمراکزشخصی سازی کارت ها، یک ریدر کارت موجود است که به منظور بارگذاری اطلاعات در تراشه مورد استفاده قرار می گیرد و نیز یک چاپگر کارت که به منظور درج عکس ها و اطلاعات در قسمت جلویی کارت به کار می رود. گاهاً پیش می آید که مرکز شخصی کردن کارت و مرکز ثبت نام در یک مکان متمرکز باشند، که در این مراکز از سیستم پردازش متمرکز یا غیرمتمرکز برای صدور و شخصی سازی کارت استفاده می شود.

۴,۲) ریدر کارت (Card reader)

از ریدر برای ایجاد ارتباط با کارت هوشمند استفاده می شود که درواقع یک رابط بین کارت و سیستم میزبان است. ریدرهای کارت توان لازم را فراهم کرده و زمان بندی ICC ها را انجام می دهند و با هردو روابط تماسی و بدون تماس می توانند ارتباط برقرار کنند.

۵,۲) رابطه هایی برای ارتباط با پایگاه های داده قبلی (Interfaces to legacy Databases)

بیشتر آژانس ها از سیستم های قبلی موجود برای شخصی کردن کارت های هوشمند بوسیله داده ها استفاده می کنند.

از این رو اجزای مهم ساختار، پلت فرم رابط هایی از سیستم های قبلی هستند که برای ایجاد ارتباط با پایگاه داده مرکزی دارنده کارت یا مراکز صدور کارت بکار می روند.

فصل سوم : ساختار مدیریت چرخه دوام کارت (Card life cycle management architecture)

در هر سیستم کارتی قوانین و وظایف باید مشخص شوند و سیاست ها و روش ها در تمام زمینه های مدیریت کارت نظیر تهیه و خریداری کارت ها، کنترل موجودی، شخصی کردن کارت، صدورکارت، جایگزین کردن کارت و مدیریت کاربردی اینچنینی توسعه یابند.

هنگام استفاده از کارت هوشمند در یک پروژه ، سه مرحله ای که در مدیریت چرخه دوام فرایند مدیریت کارت باید مورد توجه قرار بگیرند عبارتند از: مرحله پیش از صدور ، مرحله صدور ودرآخر مرحله پس از صدور.

شرکت ها و مراکزی که از پلت فرم کارت هوشمند استفاده می کنند با چالش های زیر رو به رو هستند:

۱,۳) خریداری کارت ها (Cards procurement)

صادر کننده کارت، کارت ها را از یک یا چندسازنده خریداری می کند. درصورتی که شرکت وابستگی خاصی به فروشده نداشته باشد می تواند در بازار از قیمت پایین تر و رقابتی تر بهره مند شود.

۲,۳)ارزش دهی اولیه کارت ها (Cards initialization)

ارزش دهی اولیه فرایندی است که در آن مجموعه ای از کارت ها توسط اطلاعات یکسان برای تمام اعضا مجموعه برنامه نویسی می شوند(برای مثال، ساختار فایل). ارزش دهی همچنین ممکن است شامل مرحله

چاپ کردن اطلاعات یکسان نظیر یک لوگو بر روی مجموعه ای از کارت ها باشد. این عملیات معمولاً قبل از ارسال کارت توسط سازنده کارت صورت می گیرد ولی گاهاً به هنگام شخصی کردن کارت ها در هنگام صدور کارت نیز انجام می شود. هنگام فرایند ارزش دهی اولیه، فروشنده می تواند اعمال زیر را انجام دهد:

- بارگذاری سیستم عامل در ROM
- تخصیص بخش های حافظه روی تراشه
- بارگذاری شماره سریال اختصاصی روی ROM
- تولید کلیدهای امنیتی
- انجام عملیات مربوط به عضویت درآوردن کارت که توسط شرکت یا نهاد استفاده کننده، درخواست می شود.

۳,۳) شخصی کردن کارت ها (Cards personalization)

شخصی کردن در پایان فرایند ساخت انجام می شود که درآن داده ها روی سطح کارت چاپ می شوند، نوار مغناطیسی کدگذاری می شود و داده ها برنامه نویسی شده و درتراشه ای قرار می گیرند که به دارنده یک کارت اختصاص شده است. شرکت یا سازمان با بکارگیری وسایل مختلف اطلاعات لازم را جهت فرایند شخصی کردن کارت جمع آوری می کند که بسته به تجهیزات هر سازمان متفاوت است. انتقال اطلاعات از سیستم های قدیمی موجود، روشهای تحت web برای جمع آوری داده و مصاحبه با کارمندان نمونه هایی از تکنیک های مورداستفاده برای بدست آودن داده های مورد نیاز برای شخصی کردن کارت می باشند.

پس از جمع آوری اطلاعات، از رابط ها برای وارد کردن داده ها به پایگاه داده هوشمند و یا پایگاه داده قدیمی استفاده می شود. یک رابط اتومات توانایی کاهش خطاهای دستی را دارد. امنیت فاکتور مهم دیگری است که باید مد نظر قرار گرفته شود. انتقال داده به صورت ایمن بسیار حساس و با اهمیت است خصوصاً در صورتی که از رابط های اتومات جهت انتقال داده های شخصی کردن کارت بین پایگاه داده های هوشمند یا نسل قبلی استفاده شود.

گاهاً از روش رمزگذاری برای حفاظت از انتقال داده های حساس میان شبکه های باز استفاده می شود. بسته به کاربردی که درکارت بارگذاری می شود، فرایند شخصی کردن کارت می تواند ترکیبی از چند عمل زیر باشد:

- رمز گذاری نوار مغناطیسی
- رمزگذاری بارکد
- بارگذاری نرم افزار کاربردی، اطلاعات دموگرافیک اصلی و/یا قراردادن کلیدها در تراشه
- چاپ گرافیک های کارت
- چاپ عکس و تصویر امضا روی کارت
- چاپ داده و دموگرافیک روی کارت

- چاپ دیگر اطلاعات مشخصه ی شرکت، در کارت

به عنوان بخشی از پروسه ی نام نویسی و ثبت نام برای هر کارت و فرایند شخصی سازی کارت ها، آژانس یا صادرکننده کارت طراحی شده، برای پیاده سازی هر استراتژی مناسب مورد نیاز و با توجه به شرایط خاص هر آژانس بخشی از اعمال زیر انجام می دهد.

- ثبت عکس دیجیتالی کارمندان با استفاده از سیستم عکسبرداری دیجیتال
- ثبت امضای دیجیتالی کارمندان با استفاده از وسایل ثبت امضای دیجیتالی
- ثبت مشخصات بیومتریک کارمندان با استفاده از وسایل ثبت مشخصات بیومتریک
- ثبت داده های دموگرافیک برای نگه داری در پایگاه داده دارنده کارت و بارگذاری این اطلاعات دموگرافیک در تراشه
- وارد کردن digital certificate و attribute certificate درکارت

۴,۳) صدور کارت ها (Cards issuance)

فاز توزیع کارت های شخصی شده بین دارندگان کارت را مرحله «صدورکارت» گویند. بسته به ساختار سازمانی آژانس ها و تجهیزات مورد نیاز برای برنامه نویسی کارت هوشمند، یک فروشنده عمل شخصی سازی وچاپ کارت های شناسایی هوشمند را در یک مکان مرکزی برای توزیع کلی کارت ها انجام می دهد. آژانس هایی که از لحاظ جغرافیایی پراکندگی بیشتری دارند، بیشتر تمایل به استفاده از روش های صدورکارت غیر متمرکز دارند، با این وجود مقوله امنیت عاملی تعیین کننده در روش صدور کارت توسط آژانس است. پیش از صادر شدن مجوز صدور کارت ، ویژگی های دارنده کارت جهت ارائه اسناد لازم برای تایید خصوصیات و وضعیت شغلی که بتوان آن را با پایگاه داده شخصی آژانس مقایسه کرد مورد نیاز است. برای برخورداری از سطح امنیت بالاتر،آژانس وضعیت فعلی دارنده کارت را با یک عکس و/یا مشخصه بیومتریکی که قبلاً در پایگاه داده شخصی جمع آوری شده، مقایسه می کند. کاربردهایی که روی کارت شناسایی هوشمند بارگذاری می شوند با توجه به مسئولیت و وظیفه فرد دارنده کارت متفاوت است. تمام دارندگان نیاز به یک کارت برای شناسایی بصری ودسترسی فیزیکی به محل خدمت و حوزهء مسولیت خود دارند.در شخصی کردن کارت، صدور کارت و روشهای مدیریت کارت بایدامکان ضبط و نگهداری اسناد مربوط به مجوزهای در نظر گرفته برای هرکارمند در نظر گرفته شود.

۵,۳)جایگزینی کارت ها(Cards replacement)

تعویض کارت فرایندی است که درآن در مواردی نظیر سرقت، گم شدن وعیب فنی ، کارت جدید جایگزین می شود. هنگامی که گزارش می شود که یک کارت گم شده است، یا مورد سرقت قرار گرفته است و یا

دچار نقص فنی شده است، اداره صدور با لغو certificate های موجود درکارت ،کارت را غیر فعال کرده وکارت مورد نظر را در لیست کارت های غیر مجاز قرار می دهد که معمولاً به این لیست hot-list می گویند. هنگامی که کارت جایگزین صادر می شود باید تمام امتیازات ، داده ها، کلیدهای دسترسی سیستم که درکارت قبلی موجود بوده به کارت جایگزین منتقل شوند. همچنین باید نشان داده شود که کارت، کارت المثنی است. معمولاً آژانس یا صادر کننده ی کارت طراحی شده، مسئولیت صدور کارت جایگزین (المثنی) را برعهده می گیرد. درفرآیند صدور کارت المثنی اعمال زیر معمولاً انجام می شود:

- اقدام به پیش تولید
- بررسی کارت های موجود در hot-list
- لغو Certificate ها
- زمان لازم برای غیر فعال شدن کارت های موجود در hot-list پایگاه داده .
- مسئولیت شخصی برای قفل کردن و یا بازکردن قفل ها
- خارج کرن کارت های موجود در hot-list از لیست
- تولید کلیه ها یا الگوهای بیومتریک جدید در صورتیکه کارت دارای attribute certificate یا digital certificate باشد
- زمان لازم برای صدور مجدد کارت و غیر فعال شدن کارت قبلی
- درصورتی که کارت داری کیف پول الکترونیکی باشد، بازگراندن میزان موجودی قبلی به کارت جدید.

۶,۳) بلاک کردن یا خارج کردن کارت از بلاک (CARD block / unblock)

هنگامی که گزارش می شود که یک کارت به سرقت رفته یا گم شده است ، کارت مورد نظر باید سریعاً غیر فعال شود تا افراد مجاز نتوانند از امکانات کارت استفاده کنند . یک آژانس باید توانایی قراردادن کارت هایی که گم می شوند، به سرقت می روند و یا دارای عیب ونقص فنی هستند را در hot-list داشته باشد و certificate های روی کارت را غیر فعال نماید. به علاوه سازمان های که به نحوی با این کارت در ارتباط هستند باید سریعاً از غیر فعال شدن کارت مطلع شوند. همینطور آژانس ها باید به محض صدور کارت المثنی کارت را از حالت block خارج نمایند. برای مثال هنگامی که PIN اشتباه توسط دارنده کارت بوسیله داده می شود و کارت block می شود ، این امکان باید وجود داشته باشد تا کارت توسط دارنده کارت از حالت block خارج شود(بدون نیاز به مزاجعه فرد به صادرکننده کارت).

در آخرینمرحاه ی تولید کارت وهنگام شروع به کار کارت ، کد ویژه از بلاک خارخ کردن کارت تولید شده ، به رمز در آورده می شود و سپس در سیستم کارت ذخیره می شود .

۷,۳) باز نشاندن PIN (PIN reset)

دارنده کارت باید قادر به بازنشاندن PIN خود بدون نیاز به مراجعه به مرکز صدور کارت شناسایی هوشمند باشد. بسته به تکنولوژی به کار گرفته شده در کارت ، روشهای باز نشاندن PIN متفاوت است. یک روش استفاده از رابط گرافیکی کاربر است که به کاربر این اجازه را می دهد تا بعد از بررسی صحت و درستی PIN قبلی ، PIN جدید را جایگزین کند. یک روش دیگر استفاده از پرتابل شبکه موجود در سیستم مدیریت کارت است. با استفاده از این روش بعد از تایید هویت دارنده کارت در وب سایت ، کاربر به صفحه مربوط به باز نشاندن PIN هدایت شده، جایی که PIN از طریق وسایل رومیزی مانند رایانه های های شخصی ممکن است آن طوری که کاربر انتظار دارد انجام نشود. با این حال شرکت ها باید روش هایی برای سرویس دهی به دارندگان کارت ارائه کنند که رضایت خاطر و آسودگی مصرف کننده را به همراه داشته باشد .

۸,۳) مدیریت certificate (Certificate management)

به عملیات صدور و بعد از صدور در کارت های هوشمندی که از PKI استفاده می کنند اطلاق می شود. certificate authority یا certification authority که معمولاً به آن ها CA می گویند ، دو بخشی هستند که به هیچ عنوان از تکنولوژی کلید عمومی برای تبادلات مالی دیجیتالی استفاده نمی کنند . CA به عنوان یک شخص ثالث مورد اطمینان که اعتبار یک کلید عمومی را ضمانت می کند ، سبب سهولت درانجام تبادلات درخواستی می شود. وظیفه دپارتمان CA نگه داری certificate های PKI و کلید هایی است که توسط پرتال یا سیستم صدور در کارت شناسایی هوشمند قرار داده می شوند. CA برای ساخت ، نشان گذاری و انتشار یک certificate دیجیتالی از کلید محرمانه CA استفاده می کند.

یک Certificate دیجیتالی، یک مجوز الکترونیکی است که به منظور بررسی امضای یک فرد و رمز گذاری اسناد بکار می رود و نیز از بی عیب و نقص بودن تبادلات محافظت می کند. برای ساخت یک Certificate دیجیتالی ، ابتدا CA هویت شخص را تشخیص داده و بعد از اطمینان از اینکه شخص کلید محرمانه را دارا می باشد ، آنگاه CA باید دیگر اطلاعات مورد نیاز در بقیه موارد در مورد شخصی را داشته باشد تا به ساخت Certificate اقدام کند.

مدیریت Certificate هم جزء مراحل بعد از صدور کارت است. دارندگان کارت باید توانایی درخواست یک Certificate یا به روز کردن Certificate را بعد از صدور اولیه و هنگام موارد زیر داشته باشند.

- CA هنگام صدور اولیه در دسترس نباشد.

- دریافت کننده کارت هنگام صدور اولیه کارت دارای آدرس E-mail نباشد و یا آدرس E-mail دارنده کارت بعد از صدور اولیه تغییر کند.

۹,۳) مدیریت کلید (Key management)

مدیریت کلید یک بخش جدایی ناپذیر و بسیار حیاتی در حوزه برنامه نویسی مدیریت کارت است. هر فردی که تصمیم به اجرای برنامه کارت هوشمند داشته باشد باید منابعی در دسترس داشته باشد تا به درک کامل و جامعی از کلید های کارت برسد.درک چگونگی استفاده از این کلیدها بسیار مهم است، بخصوص اگر سیستم کارت تصمیم به کار کردن با بیشتر از یک نهاد یا سازمان داشته باشد. کلید ها اسرار مربوط به سیستم را نگه داری می کنند و اگر به درستی مدیریت نشوند ، یکپارچگی سیستم بی نقص ، شبه برانگیز شده و در نتیجه بی استفاده و یا غیر قابل استفاده می شود .

مدیریت کلید فرآیندی است که بوسیله آن کلید های رمز گذاری شده تولید و نگه داری می شوند. یک واسطه بین سیستم مدریت کارت و سیستم مدیریت کلید ، انتقال کلید ها را به سیستم مدیریت کلید بسیار آسان می کند در سیستم مدیریت کارت می توان از این کلید ها برای ایجاد امنیت در کارت های هوشمند استفاده کرد .

مدیریت کلید فرآیند کنترل تولید کلید ، ذخیره کلید ، توزیع کلید ، استفاده از کلید و خرابی و نقص کلید است عملیات مدیریت کلیه شامل مواردی می شود که در شکل زیر امده است .

وظیفه	عملیات
- بررسی موثق و رسمی - کاربرد - ثبت تراشه و فعالسازی	■ ثبت نام
- بارگذاری درخواست کاربرد و حذف مجوزها - درخواست مجوز از CA - درخواست جفت کلید از ماژولهای سخت افزار امنیتی (HSM)	■ در خواست تولید کلید ومجوز
- دارای تجهیزات امنیتی مخصوصی است که باید مد نظر قرار شوند	■ ذخیره کلید ومجوز

وظیفه	نوع کلید کارت
_OP به منظور محافظت از عملیات مدیریت کلید در کارتهای تفسیری مبنای جاوا و نیز کنترل عملیات کارت مورد استفاده قرار میگیرد	■ کلید Open platform(OP)
- کنترل READ AND WRITE داده ها را انجام میدهد	■ کلید حامل
- از کلیدهای موقت است که هنگام انتقال کارتهای ایمن میان سازنده و صادرکننده کارت از آن استفاده میشود	■ کلید های انتقال دهنده
- امکان بازنشاندن PIN را فراهم میکند	■ کلید از قفل خارج کردن PIN

شکل ۱۵. عملیات کلید مدیریت

در مرحله پیش از صدور در مدیریت چرخه دوام ، سازنده کارت ۳ مجموعه کلید به نامهای کلید های حامل، شاه کلید ها و در نهایت شاه کلید open platform را در کارت قرار می دهد. شاه کلید op توسط سازنده کارت در کلید حاصل قرار داده می شود تا برای صادر کننده کارت ارسال شود. صادر کننده مجموعه کلید را مقدار دهی کرده تا در ماژول سخت افزاری امنیتی صادر کننده کارت قرار بگیرد و کلید های صادر کننده کارت تولید شوند. در فاز صدور کارت ، جفت کلید ها در کارت هوشمند در صورت لزوم بوسیله Signature key ، یک E-mail یا ID تولید می شوند. سایر فعالیت هایی که در مدیریت چرخه دوام باید

مورد توجه قرار بگیرد در صورت استفاده از signature key یک E-mail یا ID دیگر پیچیده و گیج کننده به نظرنمی آیند .

دراین مرحله از صدور کارت شناسایی هوشمند آژانس باید تمهیدات لازم برای به روز کردن کلیدهای کارت هوشمند ، جایگزین کردن PKI certificate ، تولید دوباره Signature Key، رمز گذاری جفت کلید ها وامکان باز نشاندن PIN را در صورت لزوم پیش بینی کند .

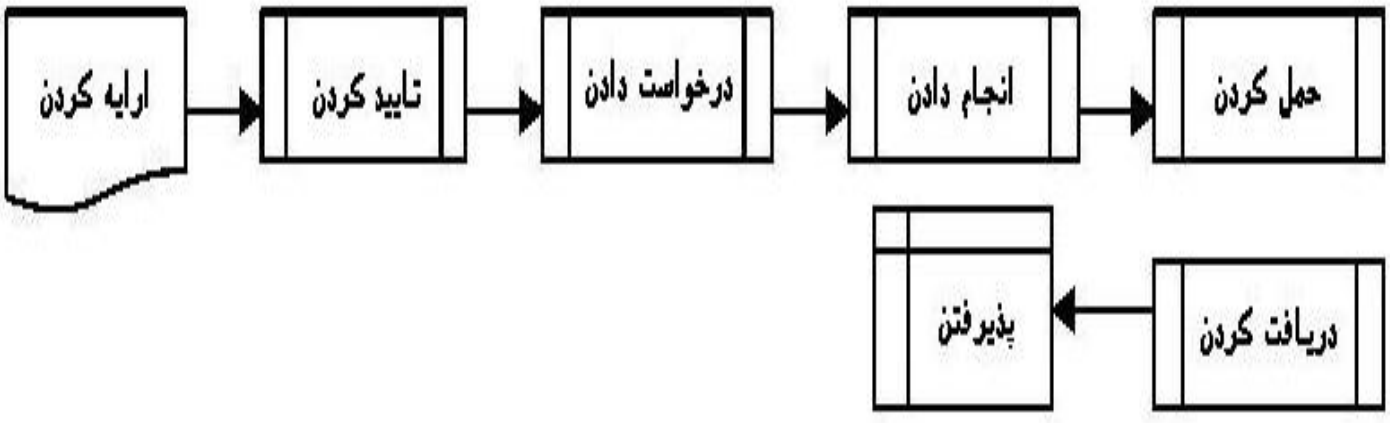
۱۰,۳) مدیریت پایگاه داده دارنده کارت

(Cardholder database management)

آژانس باید آرشیوی از تمام کارت های صادره شده داشته باشد. در این آرشیو شماره سریال کارت یا شناسنه منحصر به فرد برای ارتباط با دارنده کارت در نظر گرفته می شود. همچنین عکس دیجیتالی، تصویر امضاء فرد،digital & attribute certificate و دیگر اطلاعات مربوط به تمام کاربردهای موجود در کارت ذخیره نگه داری می شود. این آرشیو امکان انتقال تمام امتیازات مجاز موجود در کارتی که گم شده یا به سرقت رفته یا دچار نقص فنی شده را به کارت المثنی فراهم می کند .

۱۱,۳) کنترل موجودی کارت (Card inventory control)

موجودی ذخیره شده در کارت هوشمند باید در یک محیط ایمن نگه داری شود. آژانس یا صادر کننده کارت طراحی شده ، شماره سریان کارت های دریافتی را در فهرست اموال ثبت می کند ، که توسط خصوصیات و ویژگی های مرحله قبل از انتشار آژانس معین و مشخص می شود. کارت ها باید در مکانی مطمئن که محدودیت دسترسی به اسناد وجود داشته باشد نگه داری شوند. دیاگرام نشان داده شده در شکل زیر مراتب چرخه دوام را نشان می دهد



- ☐ نگه داری شماره کارت های دریافتی در فهرست کارت ها
- ☐ نظارت بر رده های فهرست کارت ها و درخواست کارت جایگزین از سازنده کارت
- ☐ به روز کردن فهرست کارت ها هنگام خراب شدن یا برگشت خوردن کارت
- ☐ پشتیبانی از پایگاه داده کارت های توزیع شده که جزئیات کارت های صادر شده بوسیله آژانس در ماه و در سال در آن موجود می باشد که این شامل وضعیت کارت ها و تراشه های دارای عیب و نقص نیز می باشد .

در طول چرخه دوام کارت ، اطلاعات فهرست کارت ها را می توان از سیستم فروشنده به سیستم آژانس منتقل کرد. سیستم فهرست موجودی کارت را می توان با سیستم مدیریت کارت ترکیب کرد.

۱۲,۳) ارائه خدمات به دارندگان کارت

(Card holder services)

آژانس یا صادر کننده کارت های طراحی می شده باید برای پلت فرم کارت کارت هوشمند ، مرکز پشتیبانی خدمات مصرف کنندگان را در نظر بگیرد که معمولاً تماس با این مراکز رایگان است و هزینه های تماس توسط آژانس پرداخت شده است. برای ارائه خدمات به دارندگان کارت ، آژانس واحد پاسخ گویی خودکار را تدارک می بیند یا این عمل توسط نمایندگی هایی که برای ارائه خدمات به مصرف کنندگان در نظر گرفته می شوند انجام می شود. از مراکز خدمات پس از فروش انتظار می رود اعمال زیر را انجام دهد .

- ☐ گزارش کارت های مفقودی ، سرقتی ، خراب و باطل
- ☐ گزارش عیب و نقص فنی یک کارت
- ☐ گزارش استفاده از کارت های غیر مجاز یا موارد رخنه در سیستم امنیتی
- ☐ گزارش داده های به روز شده (نظیر تغییر اسم ، تغییر آدرس و...)
- ☐ تهیه اطلاعات لازم برای پشتیبانی از کاربردها و خدمات کارت
- ☐ سفارش کارت جایگزین

آژانس باید موارد زیر را به شکل های مختلف به دارندگان کارت ها آموزش دهد

- ☐ استعمال عمومی کارت
- ☐ استعمال کاربردی کارت
- ☐ دستور العمل محافظت از کلید ها و امنیت کارت
- ☐ اختفاء قفل حفاظتی

فصل چهارم : امکانات کارت های هوشمند برای استفاده در آژانس ها

(Capabilities of the smart cards for use in agencies)

امکانات توسعه یافته آژانس های عرضه کننده کارت های هوشمند منجر به ابداع تکنولوژی صدور ID قابل حمل شده است که برای کاربران دسترسی ایمن به کاربردهای متنوع را فراهم می کند. جدول زیر مثال هایی از عملیات و کاربرد

عملیات و کاربردهای کارتهای هوشمند	
کاربردها	عملیات
■ شناسایی ابتدایی ■ شناسایی مبسوط ■ مجوزها	شناسایی : بررسی هویت با نمایش داده‌های دموگرافیکی،عکس یا بیومتریک های ذخیره شده؛ امکان بکارگیری فرآیند بررسی هویت خودکار توسط ربدر ایجاد امکان تصدیق هویت چند عاملی
■ پارکینگها ■ ساختمانها محیط های امنیتی	کنترل دسترسی فیزیکی : بررسی وتصدیق هویت افراد و اجازه دسترسی به مراکز فیزیکی ایمن
■ اینترنت، شخصی کردن رایانه، تلفن همراه ، بررسی و تصدیق هویت بیومتریکها،امضاء دیجیتالی،رمزهای‌عبور	کنترل دسترسی منطقی : بررسی وتصدیق هویت افراد و اجازه دسترسی به حسابها و شبکه ها
■ تراکنشهای مالی با ارزش ■ دسترسی ایمن به شبکه و اینترنت ■ دسترسی ایمن به نواحی امنیتی	بیومتریکها و امضاهای دیجیتالی: امکان بررسی تراکنشهای مالی با ارزش و کنترل با امنیت بسیار زیاد دسترسی های فیزیکی و منطقی
■ صداقت ■ تلفن ■ کتابخانه	خدمات ارزش افزوده : واحد فهرست موجودی و پیگیری: نگهداری آدرس دقیق اقلام جمع آوری شده و استفاده در خدمات In-kind
■ ثبت موارد طبی ■ فرمهای بیمه ■ تهیه کننده خدمات	ثبت و بازیابی انباره : ذخیره کردن فایل های داده و اسناد ذخیره شده که در پایانه میتوانند نمایش داده شوند یا در جمع آوری فرم های استاندارد مورد استفاده قرار گیرند
■ بدهکاری ■ اعتبار ■ E-check ■ اعتبار ذخیره شده (عوارض	خدمات مالی: محاسبه داده های مرتبط با تراکنش های مالی و نگهداری صورت وضعیت

شکل ۱۷. کاربردها و عملیات کارت های هوشمند

همانطور که در شکل نشان داده شده ابتدائی ترین موارد استفاده از کارت های هوشمند ، شناسایی، ذخیره موارد ثبت شده و بازیابی آنهاست و همچنین دسترسی فیزیکی و منطقی ایمن و ارائه خدمات مالی است.

۱,۴) شناسایی (Identification)

از کارت هوشمند می توان به عنوان یک شناسنامه که دارای مشخصه های امنیتی برای بررسی و تشخیص هویت می باشد، استفاده کرد. در وهله اول از این کارت ها می توان به عنوان یک کارت کارمندی استفاده کرد. شخص کردن کارت شامل چاپ اسم یا آژانس و دیگر داده های شناسایی اصلی نظیر قد ، وزن ، رنگ چشم ، تاریخ تولد و یا کد امنیتی می شود. امضاء یا عکس دیجیتالی را می توان روی تراشه ذخیره و از ترمینال های مجاز دسترسی انجام شود. اطلاعات و داده های دارنده کارت (نظیر اسم و عکس دیجیتال) را می توان در تراشه ذخیره کرد و با استفاده از ترمینال دسترسی مجاز انجام شده و به فرآیند بررسی هویت خودکار کمک کرد .

کارت های هوشمند گاهاً از سیستم تشخیص هویت چند-فاکتوری بهره می برند. به عنوان مثال تراشه با بهره مندی از Certificate دیجیتالی دارنده کارت که حاوی کلید عمومی است، میتواند از سیستم تعیین هویت ایمن تری برخوردار شود. Certificate دیجیتالی مشخصات دارنده کارت رادر کنار کلید عمومی قرار می دهد. کارت های هوشمند همچنین از یک کلید خصوصی نگه داری می کنند که در مواردی نظیر امضای دیجیتالی اسناد الکترونیکی و معاملات الکترونیکی مورد استفاده قرار می گیرد . از کارت های هوشمند برای نگه داری الگوهای بیومتریکی که به منظور احراز هویت دارنده کارت و تطابق یک اسکن زنده از یک مشخصه بیومتریکی فرد (نظیر اثر انگشت یا اسکن عنبیه) با الگوی موجود در کارت استفاده می کنند، بهره می برند. بدین سان کارت می تواند ایمنی بسیار بالایی را ارائه و امکان بررسی هویت و درستی مجوز دارنده کارت امکان پذیر است.

۲,۴) کارت هوشمند وامنیت ساختمانها: کنترل فیزیکی دسترسی

(Smart cards and building security: Physical access control)

کارت های هوشمند را می توان به عنوان بخشی از یک سیستم خودکار در نظر گرفت که کنترل امکان دسترسی شخص را به یک محل فیزیکی نظیر یک ساختمان ، محوطه پارکینگ ، اداره و دیگر محیط های فیزیکی انجام می دهند. گرچه کاربردهای فنی در بین سیستمکنترل فیزیکی دسترسی متفاوت است ، با این وجود سیستم هایکنترل فیزیکی دسترسی معمولاً عملیات زیر را انجام می دهند :

- ☐ عضویت دادن به کارمند
- ☐ تخصیصی امکان دسترسی
- ☐ امکان دسترسی
- ☐ به روز و باطل کردن امکان دسترسی

- ☐ تهیه مجوزهای موقت دسترسی
- ☐ تولید گزارش های دسترسی
- ☐ مدیریت hot-list
- ☐ نگه داری پایگاه داده دسترسی
- ☐ مدیریت کنترل ناظرها

در صورت یکپارچه بودن پایگاه دادهکنترل فیزیکی دسترسی یا منطقی ، در بعضی از کاربردها احتمال تداخل وجود دارد. از کارت هوشمند می توان به طرق مختلف برای بررسی هویت دارنده کارت برای سیستمکنترل فیزیکی دسترسی استفاده کرد.

- به منظور حل یک کد برای بازیابی امکان دسترسی دارند کارت از فایل های سیستم کنترل دسترسی فیزیک مورد استفاده قرار می گیرد.
- به منظور حمل یک certificate دیجیتالی برای احراز هویت دارنده کارت
- به منظور حمل الگو های بیو متریکی که جهت تطابق با اسکن زنده بیومتریک که در محل دسترسی برای احراز هویت کارت انجام می شود.

۳,۴) کارت هوشمند وامنیت IT: کنترل منطقی دسترسی

(Smart card and IT security: (logical access control))

کارت هوشمند را می توان به عنوان بخشی از یک سیستم خودکار به منظور محدود کردن دسترسی افراد به منابع یک سیستم کامپیوتری نظیر workstation ، شبکه و یا پایگاه داده مورد استفاده قرار داد. امنیت سیستم کامپیوتری معمولا شامل سه پارامتر زیر است

- امنیت داده : شامل طرح ها و پروژه های امنیتی داده است که از مکانیسم هایی نظیر به رمز در آوردن داده، جهت محافظت از اطلاعات بهره می برد.
- تعیین اعتبار و صحت اسناد : این تکنیک معمولا برای احراز هویت افراد قبل از اجاره دسترسی مورد استفاده قرار می گیرد.
- کنترل دسترسی : از تکنیک های کنترل دسترسی به منظور مدیریت و کنترل امکان دسترسی افراد به workstation ، پایگاه های داده ، سیستم های میزبان و دیگر شبکه ها استفاده می شود.

تجهیزات اصلی و پایه کنترل منطقی دسترسی در تمام سیستم ها ، تجهیزات استانداردی هستند (با وجود تفاوت در تکنیک های به کار رفته شده).

- عضویت دادن به کارمندان
- تخصیص امکان دسترسی
- به روز کردن امکان دسترسی و باطل کردن آن
- تصویق هویت فردی

- بررسی دسترسی های صورت گرفته
- تولید گزارش دسترسی

گسترش چشمگیر تمایل به دسترسی های اینترنتی منجر به بیشتر شدن نگرانی ها در مورد امنیت انتقال داده و تصدیق هویت کاربران شده است. دسترسی ایمن برای استفاده در دیگر کاربردهای دسترسی از راه دور ایمن نظیر، بانکداری بدون نیاز به مراجعه به بانک ، سیستم های بی سیم و سیستم های ماهواره ای نیز مطلوب می باشد . کارت های هوشمند یک مجوز قابل حمل و ایمن برای دسترسی های از راه دور ایمن می باشند.

۴,۴) امضاهای دیجیتال (Digital signatures)

اخیرا در مجموعه قوانین ایالات متحده آمریکا لایحه ای مورد تصویب قرار گرفته است که به موجب آن امضاهای الکترونیکی به رسمیت شناخته شد . در جهت کمک به اجرای این لایحه قانون حذف کاغذ بازی های دولتی نیز تصویب شد. قانون حذف کاغذ بازی های دولتی، رئیس اداره برنامه و بودجه را به سمت توسعه روش هایی به منظور پذیرش بیشتر امضاهای الکترونیکی هدایت کرد. به دنبال آن علاقه به استفاده از امضاهای دیجیتالی در ایالت های آمریکا بیشتر شد. شماری از ایالت ها قانون امضاهای الکترونیکی را تصویب کردند و سیاست های عمومی لازم برای پشتیبانی از رمز نویسی کلید عمومی را توسعه دادند.

رمز گذاری کلید عمومی ، استفاده از روش های پنهانی با استفاده از جفت کلید های رمز گذاری شده است، که یکی از آنها عمومی و دیگری خصوصی می باشد. هنگام اتمام عملیات رمز دار کردن با استفاده از کلید عمومی، کشف رمز نیاز به کاربردهایی مشابه کلید خصوصی دارد و بالعکس . سیستم های رمزی کلید عمومی ، طرح های تصدیق هویت را که در آنها یک رمز بدون نیاز به فاش شدن مورد بررسی قرار بگیرد را ممکن می سازند. پس از اینکه امضاهای دیجیتالی به وسیله مولفه های کلید خصوصیِ جفت کلید عمومی / خصوصی تولید شدند، کلید عمومی مشابه برای بررسی صحت امضا به کار می رود. مسلما کلید خصوصی یک کاربر هرگز در اختیار شخص دیگری قرار نمی گیرد. از این رو یک رابطه قوی بین شناسایی کاربر و کاربرد کلید خصوصی وجود دارد.

یک امضا دیجیتالی روی اسناد الکترونیکی مشابه یک امضا دستی روی اسناد چاپ شده است. این امضا داده ای غیر قابل جعل است (در عمل جعل ان غیر ممکن و گاها بسیار دشوار است) که نشان دهنده اسم شخص یا در غیر اینصورت موافقت ضمنی فرد با اسنادی که امضا شده اند، می باشد.

یک امضا دیجیتالی در واقع سطح بالاتری از امنیت را نسبت به امضاهای دستی فراهم می کند. دریافت کننده ی اسنادی که امضای دیجیتالی شده اند اطمینان دارد که:

- اسناد مستقیما از طرف شخصی که آنها را امضا کرده است دریافت شده است.
- بعد از امضا کردن در محتویات اسناد از روی عمد یا به طور تصادفی تغییری ایجاد شده است.

به علاوه امضاهای دیجیتالی را نمی توان انکار کرد و کسی که اسناد را امضای دیجیتالی کرده است نمی تواند ادعا کند که امضای او جعل شده است و او اسناد را امضا نکرده است. به طور کلی امضای دیجیتالی بررسی و تصدیق درستی پیام دیجیتالی را امکان پذیر می کند و نیز این اطمینان را به دریافت کننده می دهد که شخص امضا کننده آن را فرستاده و در نهایت بی عیب و نقص و جعلی نبودن پیام احراز می گردد. امضاهای دیجیتالی با تکیه بر رمز نگاری کلید عمومی و استفاده از زیر ساخت های کلید عمومی انجام می شوند. برای مثال هنگامی که محمد اسنادی را امضای دیجیتالی می کند، کلید عمومی و اسناد را در کنار هم قرار می دهد (یا گاها فقط اسناد را). محاسبات ترکیبی روی ترکیب حاصل برای تولید یک عدد منحصر به فرد انجام می شود که در نهایت امضای دیجیتالی پدید می آید. هنگامی که یک سند الکترونیکی از این روش استفاده می کند، خروجی یک امضای دیجیتالی منحصر به فرد است.

تائید شدن امضا فقط نیاز به داشتن کلید عمومی دارد. بنابراین محمد یک پیام را با تولید یک امضا که فقط خودش می تواند آن را تولید کند امضا می کند و دیگران می توانند تشخیص دهند که این امضای محمد است و امضای او را نمی توانند جعل کنند. استفاده از امضای دیجیتالی اساس تجارت الکترونیکی ایمن است و در کل زیر بنای ارائه خدمات الکترونیکی است.

مراحل ایجاد و انتقال موفق یک سند امضا شده دیجیتال که در آن از رمز نگاری کلید عمومی استفاده شده است در زیر آمده است

محمد ، فرستنده پیام ، ابزار : سیستم کامپیوتر شخصی

- پیامی جهت ارسال به علی ایجاد می کند
- استفاده از یک عملیات ترکیبی برای ایجاد یک خلاصه پیام (امضای دیجیتالی)
- به رمز در آوردن پیام اصلی و همینطور خلاصه پیام توسط کلید خصوصی
- ارسال پیام رمزی و امضای دیجیتال به سیستم علی

علی ، دریافت کننده پیام ، ابزار : سیستم کامپیوتر شخصی

- کشف رمز پیام با استفاده از کلید عمومی محمد.
- کشف رمز امضای دیجیتای به وسیله کلید عمومی محمد برای به حالت اول در آوردن خلاصه پیام.
- به کار بستن سیستم عملیات ترکیبی، مشابه عملیاتی که محمد با پیام اصلی انجام داده است .برای به دست آوردن یک خلاصه پیام
- مقایسه ی پیام خلاصه ای که در سیستم شخصی علی موجود است با خلاصه پیامی که از سیستم محمد دریافت شده است.

در صورت وجود تطابق صحت امضای دیجیتال محرز می شود.در پایان علی اطمینان دارد که:

۱.پیام از کامپیوتار محمد دریافت شده است.

۲.پیام در فرآیند انتقال دچار تحریف نشده است.

۵,۴) بیومتریک ها و کارت های هوشمند

(Biometrics and smart cards)

دسترس ایمن به ساختمان ها ، اطلاعات ، وجوه بانکی و یا مدارک دیگر بر ترکیبی از دو مفهوم استوار است

۱- شما چه چیزی دارید ؟ ۲- شما چه چیزی می دانید ؟

امنیت عابر بانک ها بر مبنای دو اصل شما چه چیزی دارید -کارت- و شما چه چیزی می دانید -PIN- استوار است. این نوع امنیت برای چنین مراکزی که مقادیر زیادی وجه نقد در آنجا وجود دارد با توجه امکان ثبت ، ذخیره یا سرقت PIN ناکافی و ناکار آمد است. در شرایطی که نیاز به امنیت بیشتر احساس می شد تجهیزاتی بر مبنای سوال شما چه کسی هستید ؟ ابداع و مورد استفاده قرار گرفتند که به وسیله یک مشخصه بیومتریکی مانند اثر انگشت می توانست پاسخ سوال فوق را جواب بدهد. سنجش یک مشخصه بیولوژیکی منحصر به فرد برای بررسی هویت ادعا شده توسط یک فرد به وسیله یک دستگاه خودکار انجام می شود.

بیومتریک یک ویژگی رفتاری یا بیولوژیکی یک شخص زنده که قابل اندازه گیری باشد، است که خصوصا جهت شناسایی یک شخص یا بررسی یک شناسه ادعا شده مورد استفاده قرار می گیرد. از آن جا که یک بیومتریک به طور بی همتایی به یک فرد متعلق است خود به تنهایی عامل ساده بسیار قدرتمندی برای تصدیق هویت می باشد. یک بیومتریک را می توان با یک رمز عبور یا یک وسیله جهت اجازه ورود (نظیر یک کارت هوشمند) برای داشتن بررسی هویت دو-عاملی بسیار قوی و ایمن ترکیب کرد. گرچه این سیستمهای بیومتریکی از سال ۱۹۶۸ در دسترس هستند، ولی رشد وتوسعه عمده استفاده از آن ها در ۵ سال گذشته حاصل شده است. علم بیومتریک به طور روز افزون در سیستم های حضور و غیاب ، گمرگ و مهاجرت ، سیستم فیزیکی کنترل دسترسی، سیستم های ATM و POS و کنترل دسترسی به سیستمهای اطلاعاتی، مورد استفاده قرار می گیرند .

یک بیومتریک فیزیولوژیکی (بیومتریک فیزیکی یا بیومتریک استاتیک نیز نامیده می شود)، بیومتریکی است که بر مبنای اطلاعات نتیجه گرفته شده از سنجش آناتومی یک شخص بدست می آید. برای مثال می توان از اثر انگشت ، هندسه ، کف دست ، صورت و عنبیه نام برد. یک بیومتریک رفتاری (بیومتریک دینامیک) بیومتریکی است که بر مبنای اطلاعات بدست آمده از اندازه گیری عملی که توسط شخص انجام

می شود و مشخصاً زمان به عنوان یک معیار در آن دخیل میباشد. این عمل که مورد سنجش قرار می گیرد دارای یک شروع ، میانه و پایان است. برای مثال می توان از صدا و عمل امضا کردن نام برد. بیومتریک های فیزیولوژیکی تغییر نا پذیر هستند (به استثناء مصدومیت های شدید فیزیکی). با این حال نگرانی هایی در مورد این مشخصه ها وجود دارد. بیومتریک های رفتاری ثبات کمتری از صفات فیزیولوژیکی دارند و با ناخوشی و استرس تغییر می کنند ودر کل امنیت کمتری دارند.

آنچه در ادامه آمده است انواع مختلف بیومتریک ها را شرح می دهد که می توان از آن ها در کارت های هوشمند استفاده کرد. همچنین مطالبی در مورد یکتایی بیومتریک و نیز روشهای ضبط تصاویر و الگوها

-اسکن اثر انگشت (Finger print Scan)

این بیومتریک امروزه پرکاربردترین بیومتریک مورد استفاده در دولت ایالات متحده است وتنها بیومتریک مجاز جهت استفاده در وزارت دفاع ایالت متحده آمریکا.

اسکنرهای اثر انگشت وسایل بیومتریک موفق تجاری در سالهای اخیر بوده که در سال ۲۰۰۳ تقریباً ۵۰ درصد بازار بیومتریک جهانی را به خود اختصاص دادند (براساس تحقیقات صورت گرفته در International biometric group).

انواع گسترده ای از این نوع وسایل امروزه در دسترس هستند.

مشخصه بارز : طبق برآوردهای انجام شده امکان اینکه دو شخص دارای اثر انگشت یکسان باشند، کمتر از یک درصد ملیارد است (حتی افراد دو قلو و سه قلو نیز دارای اثر انگشت متفاوتی هستند). اگر چه اثبات قضیه فوق دشوار است ولی در طی یک قرن گذشته ، هیچ دو اثر انگشت یکسانی مشاهده نشده است. به علاوه یافته ها نشان می دهد که اثر انگشت طی ۵ ماه در شکم مادر شکل می گیرد و حتی بعد از مرگ نیز تغییر نمی کند. اثر انگشت اجسادی که به خوبی مومیایی شده بودند با وجود گذشت بیش از ۲۰۰۰ سال از مرگ آنها بطور حیرت آوری بدون تغییر بود .

ضبط تصاویر : تصویر اثر انگشت را می توان با یکی از ۴ تکنولوژی زیر ثبت کرد:

- ☐ نوری
- ☐ خازنی (سیلیکون)
- ☐ حرارتی (سیلیکون)
- ☐ فرا صوتی

اکثر شرکت ها از تکنولوژی نوری استفاده می کنند ولی اغلب گرایش ها به سمت سیلیکون است.

اسکنرهای نوری که از تکنولوژی نوری استفاده می کنند، در آینده ای نه چندان دور جای خود را به سیلیکون ها می دهند .

در یک دهه گذشته ، اسکنرهای نوری پرکاربرد ترین تکنولوژی اثر انگشت به کار رفته بوده اند. تکنولوژی اثر انگشت نوری گرچه جا افتاده است ولی گران و با توجه به شرایط محیطی همیشه قابل اعتماد نیست. در عمل ، شخص انگشت خود را درمحفظه ی شیشه ای یا پلاستیکی قرار می دهد. بوسیله یک منبع نور داخلی ، اثر انگشت پرتو افکنی شده ویک دستگاه تؤام با بار[۱]، تصویر اثر انگشت را به سیگنال های دیجیتالی تبدیل می کند .

تکنولوژی خازنی (سیلیکون) بعد از معرفی رسمی در اواخر ۱۹۹۰ مقبولیت قابل توجهی بدست آوردند. اکثر تکنولوژی سیسلیکون ها یا خازن ها براساس ظرفیت جریان مستقیم (DC) است. برای مثال حسگر سیلیکون به عنوان یک جوشن خازن و انگشت فرد دیگر جوشن خازن را تشکیل می دهد. ظرفیت بین محفظه و انگشت به یک تصویر دیجیتالی مقیاس سایه زنی شده ۸ بیتی[۲] تبدیل می شود .

یک استثناء در این مورد استفاده از تکنولوژی خازن جریان متناوب (AC) است و لایه زنده پوست مورد بررسی قرار می گیرد. به طور کلی تصاویر خازنی کیفیت بهتری نسبت به انواع نوری از یک سطح کوچک تهیه می کنند. تراشه ها دقتی معادل 0.05 میلی متر یا 0.002 اینچی دارند و به اندازه کافی برای جا دادن و تعبیه در وسایلی که امکان قرار دادن تکنولوژی نوری در آن ها وجود ندارد کوچک هستند. اخیراً شرکت های بزرگ و معتبر بیشتر از انواع سیلیکونی استفاده می کنند .

در تکنولوژی حرارتی (سیلیکون)، انگشت در امتداد مستطیلی از آرایه های پیکسلی حرکت می کند که بخاطر به کار رفتن لایه pyroelectric روی سیلیکون به انتقال گرما حساس نمی باشند. یک بخش از اثر انگشت ثبت شده و چندین قسمت دیگر احیای یک تصویر اثر انگشت کامل را انجام می دهند. برای ایجاد استحکام مکانیکی بیشتر برای جلوگیری از خراشیدگی و خوردگی و مخافظت شارژ اکترواستاتیکی این تکنولوژی دارای یک پوشش سطحی ضخیم و قطور می باشد. مصرف توان در آنها بسیار کم است. این تکنولوژی تصاویر با کیفیتی تهیه می کند و قادر به ضبط اثر انگشت هایی که topopography ضعیفی دارند می باشد. این تکنولوژی Self cleaning است و با استفاده از تکنولوژی حرارتی ، حسگرها قادر به فعالیت در شرایط نا مساعد محیطی می باشند. دقت تصویر 0.05 میلی متر است (۵۰۰ نقطه در هر انیچ). با وجود استفاده از متد Swiping و جای کمی که Silicon می گیرد، استفاده از این تکنولوژی هزینه چندانی در بر ندارد.

[۱] - Charged coupled device (CCD)

[۲] - eight – bit grayscale digital image

هنوز به طور گسترده از تکنولوژی فراصوتی استفاده نمی شود. حسگر موج های صوتی را منتشر کرده و فاصله را بر اساس امپدانس انگشت ، محفظه و هوای موجود اندازه گیری می کند. استفاده های اولیه از این تکنولوژی موید این است که این تکنولوژی نوید یک تکنولوژی با دقت بسیار بالا را در آینده ای نه چندان دور می دهد.

الگوها : روش های سیستماتیک اولین بار برای تطبیق اثر انگشت با یک نمونه مشخص در قرن ۱۹ معرفی شد. یکی از این روش ها ، سیستم طبقه بندی هانری[۱] بود که براساس اگلوهایی نظیر حلقه ها، مارپیچ ها و قوس ها بدست می آمد، بود و هنوز هم امروزه برای سازمان دادن فایل های کارت های اثر انگشت از این سیستم استفاده می شود. اثر انگشت یکی از بزرگترین الگوهای بیومتریکی است(محدوده ای درخدود ۲۵۰ تا ۱۰۰۰ بایت) نکته مهم اینست که مانند دیگر تکنولوژی های بیومتریکی ، الگو فقط داده های شخصی درباره خصوصیات را نگه داری می کند و نه تصویر کامل یک اثر انگشت را و تصویر را نمیتوان مجدداً از الگو احیا کرد .

-هندسه کف دست (Hand geometry)

هندسه کف دست در حال حاضر در چند سازمان دولتی نظیر وزارت انرژی و وزارت امور خارجه ایالات متحده آمریکا مورد استفاده قرار می گیرد. سیستم های تشخیص کف دست از تکنولوژی نوری برای مکان یابی مشخصه های هندسی کلیدی کف دست به منظور بررسی هویت یک فرد بهره می برند. سیستم های تشخیص کف دست از تعداد متفاوتی از سنجش ها برای ایجاد یک الگو استفاده می کنند. این یافته ها شامل اندازه گیری طول انگشتان، تیره گی و شفافیت پوست ، ضخامت دست و قالب کف دست است. امروزه الگوی استانداردی که بتوان از آن در کارت های هوشمند استفاده کرد موجود نمی باشد.

مشخص بارز : در واقع قالب دست هر شخص با شخص دیگر متفاوت است و قالب و فرم کف دست هر شخص با گذشت زمان تغییر چندانی نمی کند. یک الگوی بیومتریکی را میتوان با سنجش خصوصیات هندسی دست یک شخص بدست آورد.

ضبط تصویر: وسایل اسکن هندسی کف دست، از روش ردیابی مکانیکی یا روش image-edgeاستفاده می کنند.در هر دوی این روش ها از یک حافظه با اطلاعات چرخان [۲] برای ثبت فرم و قالب سه بعدی دست استفاده می شود.

[۱] -Henry Classification system

[۲]- Charged – couple device

الگوها : بیش از ۹۰ مورد اندازه گیری طول ، عرض ، ضخامت و مساحت سطح دست یک شخص و/یا انگشتان برای تولید یک الگواستفاده می می شود. این نمونه یکی از کم حجم ترین الگوهاست (معمولاً بین ۱۰ تا ۲۰ بایت)

-شناسایی صورت (Facial Recognition)

هم اکنون دپارتمان های وسائط نقلیه موتوری چندایالت از ایالت های آمریکا از این تکنولوژی برای تصدیق هویت هنگام صدور گواهینامه رانندگی استفاده می کنند. شناسایی صورت بر اساس مقایسه خصوصیات و ویژگی های یک اسکن زنده از صورت در برابر خصوصیات یک الگوی ذخیره شده انجام می شود. از تکنولوژی های متعددی برای شناسایی صورت استفاده می شود. بعضی از سیستم ها از دوربین های دیجیتال موجود در بازار استفاده می کنند. این سیستم ها از الگوریتم هایی برای ایجاد یک مجموعه از اعداد مرتبط با صورت به جای استفاده از تصویر خود صورت بهره می برند. در روش دیگر از سنجش فاصله ای استفاده می شود و این عمل مثلاً با ثبت فاصله مرکز چشم تا پایین گوش یا فاصله نوک چانه تا فک بالا انجام می شود .

در روش دیگر از دو دوربین برای ثبت یک تصویر استریو از صورت استفاده می شود. در این روش تمام صورت ارزیابی شده تا صرفاً ویژگی های کلیدی و مهم صورت بدست آید. دیگر محصولات از تکنولوژی اینفرارد استفاده می کنند. به خاطر تنوع تکنولوژی های بکار رفته در محصولات مختلف ، استاندارد برای الگوی تشخیص صورت وجود ندارد.

مشخصه بارز: از نقاط ضعف این تکنولوژی ، نادیده گرفتن خصوصیات قابل تغییر مانند رنگ و حالت مو است و نیز نمی توان بین دوقلوها و یا سه قلوها تمایز قایل شود.

ضبط تصاویر: پس از ضبط یک تصویر توسط دوربین ویدیویی ، سیستم محل صورت را تشخیص داده وسیستم تصویر صورت را از مواردی دیگری که در عکس ثبت شده جدا می کند. سپس بوسیله یک نرم افزار اجزای کلی صورت نظیر چشم ها و بینی آنالیز شده و دیگر اجزای صورت نیز معین و مورد ارزیابی قرار می گیرند .

در دیگر متدهای از نگاشت سه بعدی استفاده می شود (با استفاده از یک اسکنر سه بعدی به جای دوربین) و یا تصویر برداری حرارتی از عروق خونی زیر پوست انجام می شود .

الگوها : الگوها بوسیله یکی از چند متد زیر تولید می شوند .

Eigenfaces: در زبان آلمانی eigen به معنای own است و یک تکنولوژی MIT دو بعدی می باشد و دارای تصاویری است که به طور کلی مقیاس سایه زنی روی آنها انجام گرفته است و خصوصیات برجسته یک تصویر صورت را ارائه می کند. تفاوت های eigenface در بسیاری از مواقع به عنوان اساس متدهای تشخیص صورت استفاده می شود .

تکنولوژی شبکه های عصبی : در این تکنولوژی از هوش مصنوعی استفاده می شود .

ارزیابی خمیدگی ها وانحناها : در این روش هم از نگاشت سه بعدی استفاده می شود.

گرما نگار : در این روش از تصویر برداری مادون قرمز استفاده می شود.

-اسکن عنبیه (Iris Scan)

عنبیه از شبکه های میله میله ای از بافت های پیوندی ، فیبرهای بافت های پیوندی، زائده های موئی ، فشردگی های شیار دار، حلقه ها و رنگ آمیزی تشکیل شده است. در حدود سال ۱۹۶۰ چشم پزشکان ، پیشنهاد استفاده از عنبیه به عنوان اثر انگشت نوری را ارائه کردند. این پیشنهاد بر مبنای بررسی های بالینی که نشان می داد هر عنبیه منحصر به فرد و غیر قابل تغییر است. دکتر جان داگ من[۱] عضو آزمایشگاه کامپیوتر دانشگاه کمبریج انگلستان پیشرفت های زیادی در مورد الگوریتم های ریاضیاتی متکی به تشخیص عنبیه بدست آورد .

مشخصه بارز : منحصر به فرد بودن عنبیه محرز و مسلم است. عنبیه یک بیومتریک مستحکم است که در طی زندگی یک فرد تغییر نمی کند و فرسایش و مصدومیت در آن مطرح نیست. هر چند آسیب قرنیه یا بیماری های دیگر موجب تیره و مات شدن عنبیه می شود. نظیر اثر انگشت الگوی هیچ دوعنبیه یکسان نمی باشد (حتی در دوقلوها).

ضبط تصویر : ایراداتی به عنبیه وارد است من جمله کوچک بودن این عضو (حدود ۱ سانتیمتر یا نیم اینچ) که از فاصله یک متری یا یک یاردی باید مورد شناسایی قرار بگیرد واغلب این عضو در معرض جابجایی است. علاوه بر این عنبیه پشت یک سطح خمیده ، خیس و بازتاب کننده قرار می گیرد و بوسیله مژه ، لنز ، و بازتابش پوشانده می شود و نیز تا حدودی توسط پلک چشم که اغلب پژمرده و افتاده می شود مسدود می شود. این مشکلات سبب استفاده از وسایل ضبط تصویر پیشرفته تری می شود که طبیعتاً هزینه بیشتری برای آنها باید پرداخت شود.ضبط تصویر عنبیه می تواند پسیو یا اکتیو باشد که در ضبط تصویر اکتیو فاصله کاربر باید بین ۱۵ تا ۳۵ سانتیمتر (۶ تا ۱۴ اینچ) از لنز دوربین باشد. در ضبط تصویر پسیو از لنزهای Wide استفاده می شود که بطور اتوماتیک فاصله از چشم را معین کرده و برروی چشم برای ضبط تصاویر زوم می کند. در این روش فاصله کاربر از دوربین بین ۳۰ تا ۱۰۰ سانتیمتر (۱ تا ۳ فیت) است. این سیستم کاربر پسند تر است ، گرچه هزینه بیشتری دارد .

الگوها : الگو یا کد عنبیه بوسیله کشف رمز الگوی عنبیه بدست می آید. این فرایند ریاضیاتی با اندازه عنبیه تغییر نمی کند (از این رو فاصله تصویر برداری روی آن بی اثر است) و با فراخ شدن قطر مردمک درعنبیه

[۱] - Dr . John Daugman

نیز این فرایند تغییر نمی کند. همچنین نسبت به کنتراست دریچه دوربین و سطح دریچه دوربین و سطح روشنایی غیر حساس است. برای یک توصیف خلاصه فقط نیاز به ۲۵۶ بایت برای هر الگوی عنبیه می باشد (۲۵۶ بایت دیگر یک کد عنبیه ۵۱۲ بایتی، فرآیند مقایسه را کنترل می کند).

۶,۴) سیستم های بیومتریکی (Biometric system)

هر چند تکنولوژی های بیومتریکی در اینکه چه چیزی را و چطور آن را می سنجند متفاوت هستند، تمام سیستمهای بیومتریکی طرز کار مشابهی دارند. کاربر نمونه ای بوسیله یک ابزار مانند اسکنر یا دوربین ارائه می کند. این بیومتریک برای استخراج اطلاعات در مورد یک صفت مشخصه به منظور ایجاد یک الگوی آزمایشی پردازش می شود. الگوها در واقع رشته های عددی بزرگی هستند. احیا کردن نمونه از الگو غیر ممکن است. الگو آزمایشی معادل با کد عبور کاربر است .

۷,۴) استفاده از بیومتریک ها درکارت های هوشمند

(Use biometrics in smart cards)

بسته به نوع بیومتریک ، نقش کارت هوشمند تا حدودی متفاوت است. دو استفاده عمده در کارت های هوشمند درادامه آمده است :

- **Match off-card**

در این نوع کاربرد ، الگوی ثبت شده در ابتدا روی کارت بار گذاری شده و سپس از طریق کارت هوشمند ، هنگامی که یک سیستم بیومتریکی خارجی آن را طلب نماید ، بوسیله رابطه های تماسی یا بدون تماس عرضه می شود. سپس تجهیزات خارجی نمونه زنده اسکن بیومتریکی را با نمونه ای که قبلاً روی کارت قرار گرفته مقایسه می کنند. واضح است که این کاربرد خطرات امنیتی احتمالی در ارتباط با انتقال الگوی ثبت شده کارت هوشمند در هر چالش بیومتریکی دارد .

ارزیابی امنیتی مناسبی باید به کار گرفته شود تا محرمانه ماندن الگوی در اختیار گرفته شده ، به خطر نیفتد. با این تکنیک کارت خوشمند یک الگو را ذخیر می کند. نسبت به نوع اطلاعات بیومتریکی شناخت زیادی ندارد و در هر حال قادر به پردازش آن هم نیست. این روش کاربردی مناسب برای انواع مختلف کارت هایی است که در آنها نیاز به یک سیستم هوشمند قوی می باشد. دراین تکنیک از حافظه سیم کشی منطقی وکارت های هوشمندی که بر مبنای ریز پردازنده کار می کنند استفاده شده است .

- **Match on-card**

این تکنیک کاربردی ، در ابتدای الگو های ثبت نامی را روی حافظه ایمن کارت های هوشمند ذخیره می کند هنگامی که یک تطبیق بیومتریکی در خواست می شود ، تجهیزات خارجی یک نمونه اسکن زنده جدید را برای کارت تهیه می کنند. کارت هوشمند به وسیله پردازنده حفاظت شده خود ، عملیات تطبیق را انجام داده و نتایج رادر اختیار تجهیزات خارجی قرار می دهد. در این روش از الگوهای ثبت شده اولیه محافظت می شود زیرا همواره در داخل کارت صورت می گیرد و از کارت به هیچ عنوان خارج نمی شود. از حریم خصوصی دارنده کارت نیز در این تکنیک محافظت می شود زیرا اطلاعات الگوهای بیومتریکی دارنده کارت از روی کارت هوشمند قابل دستیابی وخواندن نمی باشد. با این تکنیک می توان کارت هوشمند را به ابزاری بر مبنای ریز پردازنده که قادر است تطابق یک به یک را محاسبه کند تبدیل کرد.

۸,۴) استفاده های تجاری : (Business use)

سه کاربرد کلی سیستم های بیومتریکی به قرار زیر است

- تصدیق کاربر برای کنترل دسترسی به سیستم اطلاعاتی
- کنترل دسترسی فیزیکی
- مانیتورینگ (برای مثال زمان حضور و غیاب)

۹,۴) مزایای تکنولوژی بیومتریکی

(Biometric technology benefits)

افزایش امنیت

- اطلاعات بیومتریکی دزدیده نمی شوند ، مفقود و فراموشی نمی شوند. بوسیله مهندسی اجتماعی[۱] امکان یادداشت و ثبت این اطلاعات وجود ندارد. این اطلاعات رانمی توان با یک کاربر دیگر به اشتراک گذاشت و در نهایت فقط خود شخص قادر است که از این مجوزها استفاده کند.
- با استفاده از این بیومتریک ها ، سازمان ها با امنیت بالا قادر به شناسایی کاربران و تصدیق هویت آنان می باشند وامکان انجام معاملات سنگین با امنیت بالا که توسط کاربر از طریق یک درگاه از راه دور یا اینترنت درخواست می شود وجود دارد.
- در صورت استفاده از آن ها در کارت های هوشمند ، بیومتریک ها امنیت بالایی را برای مجوزهای PKI که روی کارت موجود می باشند فراهم می کنند.
- دیگر نیاز به ارائه یک کارت یا بیاد آوردن یک Password یا PIN توسط کاربر نمی باشد. با توجه به اینکه اطلاعات بیومتریکی مفقود، دزدیده و فراموش نمی شوند، همیشه در دسترس کاربر هستند .
- سازمان ها می توانند مانع اقتصادی وانسانی مورد نیاز برای مدیریت کد عبور را حذف کرده و خدمات دهی به مشتریان خود را ارتقا بخشند .

[۱] -Social engineering

- در صورت بهره مند شدن سازنان ها از سیستم های تشخیص عناصر بیومتریکی به جای سیستم های تصدیق هویت ساده کاربر دیگر مجبور به وارد شدن به سیستم اطلاعاتی به صورت دستی و غیر اتوماتیک نیست .

۱۰,۴) خطرات احتمالی تکنولوژی بیومتریکی

(Biometric technology risks)

نگرانی های پنهانی : کاربران ، خصوصاً مصرف کنندگانی که اغلب حقوقی هستند، بیشتر نگران ذخیره و پخش و توزیع داده های بیومتریکی می باشند. اگر یک سازمان دارای انبار مرکزی برای نگهداری الگوها باشد کابران کنترلی در توزیع و پخش این داده ها ندارند و نگرانی هایی نظیر :

- سوء استفاده از داده ها (برای مثال تبادلات غیر مجاز با دیگر سازمان ها)
- استفاده در زمینه ای غیر از زمینه ای که داده در اختیار سازمان قرار داده شده است.

در اتحادیه اروپا ، قانون حفاظت اطلاعات ثبت شده در مورد داده های بیومتریکی نیز به کار می رود. در ایالات متحده آمریکا و دیگر نقاط نیاز به یک قانون مدون نظم دهنده برای خفاظت از این اطلاعات شدیداً احساس می شود. یک راه کار برای کاهش نگرانی ها ، قرار دادن الگوهای مرجع کاربر در کارت هوشمند می باشد .

دیگر نگرانی ، ترس از تجسس و جستجو در سوابق یک فرد و نظارت بر اعمال فرد درهر لحظه است .

هنگام استفاده از یک کارت هوشمند که در آن سیستم های بیومتریکی به کار رفته است ، کارت هوشمند در قالب یک تکنولوژی امنیتی و کمک کننده مطرح می شود. کارت هوشمند توانایی تقویت یک سیستم بیومتریکی یا یک سیستم شناسایی را دارد. به این ترتیب که یک محفظه امن برای الگوهای بیومتریکی و امکان محاسبه تطبیقی بیومتریکی در کارت را هنگام قرار گرفتن کارت در دستگاه خارجی را ایجاد می کند.

۱۱,۴) نگرانی های شخصی، فرهنگی و مذهبی

(Personal , cultural and religious concerns)

استفاده از سیستم های اثر انگشت با مخالفت هایی رو به رو شد که ناشی از جنبه تبهکاری و جنایی استفاده از اثر انگشت در جرائم دادگاهی می شد. همچنین نگرانی های بیشتری در مورد جنبه بهداشتی (یک اسکنر کف دست ، باید بعد از هر بار استفاده ضد عفونی شود) و احتمال اسیب های جبران ناپذیر و در مرتبه خطرناک تر احتمال اینکه اشخاص تبهکار با قطع دست یا انگشت یک فرد به اهداف خود برسند ، وجود داشت.

در بعضی از فرهنگ ها و مذاهب حکم تحریم استفاده از سیستم های بیومتریکی صادر شده است. برای مثال ژاپنی ها تمایل چندانی به استفاده از سیستم های اثر انگشت و یا سیتسم شناسایی کف دست ، که افراد دیگر نیز از آنها استفاده می کنند ندارند .

بعضی از گروههای مسیحی بیومتریک ها را با the mark of the beast (نشانه ای برای حیوانات) که در کتاب مکاشفه یوحنا 13:16-17 آمده است مرتبط می دانند. چنین برداشت هایی موجبات نگرانی مصرف کننده ها را به دنبال داشته است.

۱۲,۴) رهنمودهای انتخاب یک بیومتریک مناسب

(Biometrics selection guidelines)

سازمان ها باید سطح امنیت مورد نیاز برای کاربردهای مورد نظر خود را معین کنند. در حالت کلی بیومتریک های رفتاری برای کاربردهای امنیتی متوسط به پایین مناسب می باشند و بیومتریک های فیزیولوژیکی برای کاربردهای امنیتی متوسط به بالا مناسب هستند. از طرف دیگر ، سازمان ها باید آگاهی کامل از اندازه و ترکیب تعداد کاربران ، وسایل مورد نیاز (تعداد باجه ها و ....) و محیط کار وسیله (داخلی یا خارجی) داشته باشند. یکی از موانع مهم در پذیرش تکنولوژی بیومتریکی مقیاس پذیری و قابلیت اداره سیستم های بیومتریکی است (خصوصاً در شبکه های تشکیلاتی غیر همگن). در سال های اخیر شماری از فروشندگان که بیشتر در زمینه های صنعتی فعالیت می کنند محصولات Authentication management infrastractuer (AMI) را برای عرضه خریداری کرده اند . نظیر دیگر وسایل تصدیق هویت میان افزار مانند محصولات Single sign on (sso) محصولات AMI از متدهای بررسی تصدیق هویت متعددی پشتیبانی می کنند و نه فقط لزوماً تکنولوژی بیومتریکی. بر خلاف محصولات SSO یک محصول AMI یک قالب مدیریتی ساده و خدمات تعیین اعتبار و صحت اسناد برای سیستم های مورد نظر چند-گانه را فراهم می کند و به سازمان اجازه می دهد از روش های متفاوتی به منظور تعیین اعتبار و صحت اسناد استفاده کند، چه به صورت ساده و یا به صورت ترکیبی.

یک سازمان در بلند مدت به دنبال به دست آوردن سود بیشتر از انتخاب یک محصول زیر ساختی خوب است و نه صرفاً انتخاب یک بیومتریک دقیق و در کوتاه مدت هنگامی که سازمان میخواهد از میان انواع بیومتریک ها یک نوع بیومتریک خاص را انتخاب کند ، باید موارد زیر در نظر گرفته شود؛

- سادگی استفاده
- دقت و امنیت (قابل اعتماد بودن و مقاومت و استحکام در برابر حملات)
- هزینه
- ذخیره الگوها

فصل پنجم : مزایای به کارگیری یک سیستم کارت هوشمند :

(Benefits of implementing a smart card system)

با توجه به نیاز به یک زیر بنای گسترده و هزینه های هنگفت مرتبط با تهیه و تدارک سیستم های کارت هوشمند، آژانس ها تمایلی به استفاده از این تکنولوژی ندارند. هر چند تغییرات زیر سبب افزایش گرایش به سمت استفاده از کارت های هوشمند شده است .

- افزایش شمار کارت های تراشه دار :

پس از ان که American Express شروع به صدور Master card و visa card کرد، کارت های تراشه دار در آمریکا بااقبال عمومی روبه رو شدند. در نتیجه بخش های تجاری نیز علاقه خود را در بکارگیری کارت های تراشه دار نشان دارند. از طرف دیگر ، انعقاد پیمان GSA Smart access ID منجر به افزایش قابل توجهی در به کارگیری کارت های هوشمند در واحدهای اداری شد. در پی سیاست حرکت به سمت تجارت الکترونیکی ، دولت سیاست خود را تمایل خود را به استفاده بیشتر از تکنولوژی کارت هوشمند نشان می داد. با افزایش شمار کارت های صادر شده و به وجود آمدن زیر ساخت های مناسب ترقی و رشد کارت های هوشمند در دنیای تجارت با سرعت بیشتری انجام شد .

- کاهش قیمت کارت ها :

با افزایش تولید کارت های صادر شده، قیمت کارت های نیز متقابلاً کاهش یافت. بسته به امکانات تعبیه شده در کارت قیمت کارت های بین ۳ تا ۱۰ دلار متغیر است (در خرید کلی). با ادامه روند افزایش تقاضا ، پیش بینی می شود که قیمت کارتها همچنان در سراشیبی سقوط قرار داشته باشد .

- کاهش زمان پاسخ گویی :

با ظهور سیستم های عامل پیشرفته (مانند Java card) و پردازش سریع تر ، در واقع زمان لازم برای خواندن داده ها از تراشه ونوشتن داده ها در تراشه کاهش یافت. این کاهش در زمان پاسخ گویی از دیگر دلایل گرایش به سمت کارت های هوشمند بود.

افزایش ظرفیت حافظه : ظرفیت حافظه به طور پیوسته از ۱ تا ۶۴ کیلوبایت افزایش یافت که در حال حاضر ۳۲ کیلوبایت ظرفیت متوسط است این افزایش ظرفیت حافظه کاربردهای کارت را افزایش داده در نتیجه دیگر نیازی به استفاده از چند کارت که دارای کاربردهای مختلف ، باشند نیست. پی آمد همه این موارد کاهش هزینه ها بود .

- حرکت به سمت کارت های چندگانه :

با افزایش امنیت و افزایش حافظه و امکانات کارت ها ، استفاده از کارت های چندگانه رونق زیادی یافت. این کارت ها تسهیلات قابل توجهی را برای دارنده کارت فراهم می کردند. شاید بیشتر از همه عامل دیگر، گرایش به سمت کارت های چند-گانه موجب ترغیب بیشتر به استفاده از کارت های هوشمند در میان نهادهایی شد که استطاعت مالی برای استفاده از پلت فرم های کارت های مجزا برای هر کاربرد به صورت جداگانه را نداشتند.

- وضع قوانین و توسعه استانداردها :

وضع قوانین و توسعه استانداردها ، سبب افزایش هماهنگی ها شد. شماری از این قوانین جدید سبب ترویج مفهوم هماهنگی شد. بعلاوه ساختار استانداردها به شکلی بود که با توجه به گام های بلندی که در زمینه صدور و اشاعه استانداردها برداشته شد ، زمینه برای همکاری مشترک کارت ها و ریدرها بوجود آمد .

بخش بعدی به آژانس ها در بررسی اینکه آیا شرایط مناسب برای بکارگیری سیستم کارت های هوشمند را دارند یا نه کمک می کند .

۱,۵) چرا بهتر است یک سیستم کارت هوشمند را به کار برد ؟

گرچه کارت های هوشمند نسبت به کارت های پلاستیکی ساده قیمت بیشتری دارند ، استفاده از یک پلت فرم کاربردی چندگانه هزینه کلی یک سیستم کارتی هوشمند برنامه ریزی شده را کاهش می دهد. صادر کنندگان کارت ها و مصرف کنندگان انتظار دارند تجربه در صدور کارت و مدیریت هزینه ها با کاهش قیمت ها، به کمک آنها بشتابد.

- ادغام : پردازش داده و اطلاعات خدمات مرکزی میان کاربردهایی که روی کارت قرار می گیرند تقسیم می شوند که در نهایت این عمل برای مصرف کنندگان تقسیم هزینه ها را در پی دارد .

- جمع آوری داده : جمع آوری و ذخیره داده ها ی معمولی در کاربردهای چند-گانه میان مصرف کنندگان تقسیم می شود
- شخصی کردن : در کاربردهای چند-گانه کارت فقط یک بار شخصی سازی و صادر می شود و دیگر نیازی به کارت های شخصی شده مجزا برای هر کاربرد نیست. این عمل منجر به کاهش هزینه برای مصرف کنندگان می شود .
- تقسیم زیرساختار : در بیشتر کاربردها هزینه تقویت و گسترش زیر ساختارها میان مالکان آن کاربرد تقسیم می شود.
- اعتماد به کارت : عملکرد و دوام کارت های هوشمند در سال های اخیر ، رشد چشمگیری داشته که در نهایت منجر به کاهش هزینه ها شده است .

درارزیابی کارت های هوشمند ، آژانس یا نهاد مورد نظر باید نقش خود را در تبدیل تجارت قبلی به تجارت الکترونیک و/یا دولت الکترونیک درک کند . اگر در محاسبات انجام شده در مورد هزینه ها ، ضربه سنگینی به آژانس تحمیل شود، راههای ارزان تر و کم هزینه تری نسبت به استفاده از کارت های هوشمند نیز وجود دارد . کارت های هوشمند مزایای ذیل را به همراه دارند:

- افزایش امنیت

یکی ازمهم ترین مزایای کارت هوشمند توانایی آن درحمل یک مجوز دجیتالی یا یک الگوی بیومتریک برای کمک به تصدیق هویت دارنده کارت است کارت هوشمند شرایط دسترسی ایمن تر به یک ساختمان ، مناطق حفاظت شده و سیستمهای الکترونیکی را فراهم می کند

- تسهیل در درسترس به ساختمانها ، متینگ ها ، کامپیوترها ، تلفن ها ، Internet , Email :

با استفاده PIN ها، بیومتریک ها یا مجوزهای دیجیتالی موجود در کارت ، کارت هوشمند به دارنده کارت این امکان را می دهد که دسترسی راحت تری به امکانات فیزیکی و سیستمهای الکترونیکی داشته باشد. اشخاص در دراز مدت توانایی به یاد آوردن رمز های عبور مختلف را ندارند و قادر به پرکردن فرم های کاغذی تکراری برای دسترسی به ساختمانها ، متینگ ها ، ارتباطات و سیستم های نیستند. برای بررسی کاغذ بازی های مرتبط با کارهای اجرایی ساعت های زیادی موردنیاز است که در صورت استفاده از کارت های هوشنند از اتلاف ساعت های بی شماری ممانعت به عمل می آید .

- ادغام تجهیزات شناسایی شخص :

کارت هوشمند یک اعتبار نامه مرکزی ساده را مهیا می کنند که همان هویت دیجیتالی شخص است. بواسطه این عمل دیگر نیازی به اینکه افراد کارت های مختلفی با خود حمل کنند و PIN های متفاوتی را به یاد بیاورند ، نیست.

- دسترسی و پرداخت ایمن و محرمانه خرید های اینترنتی :

یکی از عواملی که مانع از حرکت آژانس ها به سمت بکارگیری مبادلات الکترونیکی می شود، ترس آنها از نبود امنیت لازم برای انجام تبادلات از طریق شبکه اینترنت است. آژانس هایی که تمایل به حرکت به سوی تجارت الکترونیک دارند، در ابتدا نیاز به یک مکانیسم انتقال الکترونیکی بسیار مطمئن دارند .

- فراهم کردن فرم های الکترونیکی و کاهش پرونده های کاغذی:

گرچه بسیاری از آژنس های به آرامی به سمت استفاده از فرم الکتریکی حرکت می کنند ، خصوصاً در محیط های ادارای نیاز به نگه داری امضاهای کاغذی برای مقاصد قانونی ایجاد پرونده های کاغذی زائد و اضافی ضروری است برای ایجاد شرایطی که در آن امکان انکار عمل انجام شده بنشاد ، امضاهای دجیتالی به طور فرآیند ه ای دراسناد الکترونیکی به کار رفتعند که خود به خود سبب حذف و جایگزینی اسناد الکترونیکی بوسیله پرونده های

کاغذی می شود و در نهایت سبب حرکت آژانس ها به سمت دفاتر الکترونیکی شد امضاهای دیجیتالی بوسیله کارت های هوشمند قابلیت جابه جایی پیدا کردند .

- حسابداری خود کار :

استفاده از کارت هوشمند امکان خرید پایاپای را فراهم می کند. از این رو اطلاعات حسابداری به صورت الکترونیکی قابل انتقال است. فرم های اداری به صورت الکترونیکی توسط کارمندان کامل می شود و سپس به آسانی به سیستم های حسابداری منتقل می شود. در نهایت مانع از اتلاف وقت و سرمایه می شود .

رضایت کارمندان / آسودگی فروشندگان :

- کارمندان قادر به حمل داده های مربوط به خود در هر مکانی هستند در نتیجه دسترسی آسان تری به داده هایی که نیاز به جمع آوری فرم های ضروری دارد خواهند داشت. کارت های هوشمند انعطاف پذیری بیشتری را برای کارمندان هنگام استفاده از سیستم های کامپیوتری فراهم می کنند و به آنها اجازه می دهد دسترسی ایمن تری به سیستم های از راه دور داشته باشند. کارت های هوشمند همچنین قادر به نگهداری داده های بهداشتی و دموگرافیکی در خود هستند .

۲,۵) مزیت های نسبی کارت هوشمند در مقایسه با دیگر تکنولوژیها

(Relative merit of smart card VS alternative technologies)

شماری از تکنولوژی های تجاری موجود را در طراحی یک سیستم شناسایی می توان مد نظر قرار داد. آژانس های دولتی و نهادهای خصوصی ، ترکیبهای مختلفی از روشهای شناسایی را برای اهداف شناسایی ایمن خود مورد استفاده قرار می دهند. این بخش به بررسی انواع تکنولوژی های ID که در حال حاضر در دسترس هستند و مزایا و معایب نسبی به کارگیری سیستم های ID محرمانه مهم و حساس می پردازد .

- **مجوزهای تعیین اعتبار و صحت و اسناد اعتبار نامه ها**

(Credential documents and authentication tokens)

امروزه در اکثر ادارات و وزارت خانه های دولت امریکا ازاین نوع سیستمهای ID استفاده می شود. استانداردهای امنیتی برای ساختمانهای دولتی نیاز به مجوزهایی دارد که این مجوزها در کارت های هوشمند تماسی و یا بدون تماس و تکنولوژی های بیومتریکی تعبیه شده که اشاره به سطح امنیت در نظر گرفته شده برای یک مکان دولتی دارد.

- **کارت های کاغذی یا پلاستیکی**

(Plastic or paper cards)

کارت های ساده پلاستیکی یا کاغذی هستند که اطلاعات شناسایی روی کارت چاپ می شود (اسم ، آدرس عکس فرد) و در کاربردهای بی شماری مورد استفاده قرار می گیرند. این کارت ها در صورتی که همراه فرد باشند، مورد بررسی توسط ماموران امنیتی قرار می گیرند. به این خاطر که در شناسایی بصری به ماموران امنیتی نیاز است که تصویر شخص را تشخیص داده و در نتیجه به قضاوت فردی اعتماد می شود ، شناسایی بصری یکی از روش های شناسایی است که کمتر مورد توجه قرار می گیرد .

- **بار کد (Bar code)**

یک بار کد تصویری از خطوط با عرض های متفاوت است که آنها را می توان ضمیمه اجناس خرده فروش ها ، کارت های شناسایی ، نامه های پستی برای شناسایی یک شماره محصول ویژه یا مکان فرد به کار می روند، کرد. این کد از خطوط عمودی کنار هم تشکیل شده و فضای زیر این خطوط برای نمایش اعداد درنظر گرفته می شود.این فضا معمولاً دارای ۵ قسمت است .

Quiet zone ، کاراکتر شروع ، کاراکترهای داده (شامل کاراکتر بررسی انتخاب) کاراکتر توقف و یک Quiet zone دیگر. بارکدها می توانند اطلاعات شخص را ذخیره کنند. بارکدها روی کارت های پلاستیکی قابل چاپ هستند. بارکدهای خطی برای ذخیره داده های الفبایی عددی ساده به کارمی روند (در کاربردهای جزئی). بارکدهای دو بعدی امروزه می توانند داده های بیشتری را در یک فضای کم ذخیره کنند (تا ۱۱۰۸ بایت).

داده ها در یک بارکد ترجمه شده در مرحله چاپ روی کارت تعبیه می شوند. سپس کارت توسط یک ریدر بارکد اسکن می شود. ریدر از یک پرتو لیزر که به بازتاب خطوط و همینطور ضخامت و پراکندگی خطوط حساس است استفاده می کند. با استفاده از یک دستگاه فتوکپی استاندارد می توان به راحتی بارکد ها را کپی کرد. در نتیجه در بعضی از کاربردهایی که به سطح امنیت بالاتری نیاز دارند نمی توان از بارکد ها استفاده کرد. «پوشش» یک متد برای پوشاندن بارکدها و بالا بردن امنیت بارکدها است. چاپ کردن یک بارکد با ماشین های چاپی که دارای مقدار زیادی کربن هستند و سپس پوشاندن بارکد با جوهر سیاه فاقد کربن مانع از کپی برداری غیر مجاز از بارکد می شود و همچنان امکان خواندن بارکد توسط قلم نوری اینفرارد و یا اسکنر وجود دارد . این روش تا حدی امنیت بارکدها را افزایش می دهد.

- **کارت های نوار مغناطیسی (Magnetic stripe cards)**

این کارت ها از حدود سال ۱۹۷۰ به طور گسترده در کاربردهای مختلفی به کار می روند (از کارت های مالی اعتبار گرفته تا کارت های ترانزیت گواهینامه های رانندگان). نوار مغناطیسی در پشت یک کارت ID توسط اجزای مغناطیسی مبنای آهن ساخته می شوند و در پوششی از پلاستیک قرار می گیرد. هر جزء

مغناطیسی در نوار ، یک آهنربای میله ای بسیار کوچک است که چیزی در حدود بیست ملیونیوم یک اینچ طول دارد. هنگامی که تمام آهنرباهای میله ای در یک جهت قطبی شوند ،نوار مغناطیسی خالی است . با مغناطیسی کردن میله های بسیار کوچک چه در جهت شمال چه در جهت جنوب بوسیله یک رایتر الکترومغناطیسی که به آن اینکدر می گویند اطلاعات اطلاعات روی نوار نوشته می شود. اطلاعات شناسایی هنگام فرایند شخصی سازی روی واسطه های مغناطیسی قرار می گیرند و سپس بوسیله یک حرکت جارویی یا تعبیه و الحاق ریدر در مکان فعل و انفعال خوانده می شوند. داده های کاربر اینکد شده در نوار مغناطیسی را با استفاده از یک ریدر مغناطیسی استاندارد به راحتی می توان کپی و تفسیر کرد. همچنین داده ها را می توان به یک کارت دیگر منتقل کرد. این امکان تکنولوژی نوار مغناطیسی را تبدیل به یک تکنولوژی مناسب برای کاربردهایی که در آنها نیاز به سطح امنیت بالایی نیست ، کرده است .

- **کارت های نوری یا کارت های نوار نوری**

(Optical or optical stripe cards)

کارت های نوار نوری یک تکنولوژی استاتیک اختصاصی است که در آن از تجهیزات خارجی اختصاصی برای خواندن،نوشتن و پردازش اطلاعات ذخیره شده در وسایلی مانند دیسک های فشرده استفاده می شود. کارت های نوار نوری دریک پوشش کاغذی محافظ برای کاهش آسیب به ماتریال ذخیره شده نوری در کاربردهای معمولی نگه داری می شوند. کارت های نوار نوری با استفاده از تکنولوژی نگارش با یکبار نوشتن و بارها خواندن (Worm [1]) ، اجازه نوشتن و اضافه کردن داده ها را می دهد. ولی امکان پاک کردن و حذف داده ها وجود ندارد. این کارت ها ظرفیت حافظه غیر فرار نسبتاً بالایی دارند (چندین مگابایت) و در شناسایی ، کمک های پزشکی ، مدیریت منطقی و دیگر کاربردهایی که در آن ها نیاز به حجم زیادی از داده های ذخیره شده است از آنها استفاده می شود .

- **کارت های هوشمند – کارت های تماسی یا بدون تماس**

(Smart cards – cantact or contactless cards)

کارت های هوشمند یک تراشه کامپیوتری جاسازی شده دارند که می تواند یک ریزپردازنده یا یک حافظه داخلی یا به تنهایی یک تراشه حافظه باشد. کارت به یک ریدر با تماس فیزیکی مستقیم یا یک رابط الکترومغناطیسی بدون تماس از راه دور متصل می شود. بوسیله یک ریزپردازنده، کارت هوشمند توانایی

[1] - WORM: write once , read many

منحصر به فردی در ذخیره حجم زیادی داده دارد و به تنهایی عملیات و دستور العمل های موجود در کارت را انجام می دهند (رمزدار کردن و امضاهای دجیتالی) ویک فعل وانفعال هوشمندانه با ریدر کارت هوشمند دارد. در سرتاسر جهان از کارت های هوشمند در کاربردهای مالی ، مخابراتی (ارتباطی)، حمل و نقل ، مراقبت های پزشکی ، شناسایی پیشرفته و ایمن استفاده می شود. امروزه کارت ها ی هوشمند مبتنی بر ریزپردازنده تا ۱۲۸ کیلوبایت داده قابل استفاده را می توانند در خود ذخیره کنند. مدل های آینده از این مقدار هم بیشتر ذخیره خواهند کرد. استفاده از مکانیسم های قفل گذاری و رمز گذاری ذخیره داده روی تراشه های کارت های هوشمند بصورت بسیار مطمئن و با ایمنی بالا انجام می شود. کارت های هوشمند بوسیله محیط های محاسباتی داخلی ایمن خود عملیات پیچیده بسیار مشکلی را انجام می دهند .

Paper–Based Resources:

1. National Strategy for Homeland Security, OHS 2002.
2. National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, Interagency Report 6887-2003 Edition, Government Smart Card Interoperability Specification, Version 2.1, July 16, 2003.
3. Russell, James, Comparison of Dynamic versus Static Technology with Relation to Memory and Security, MasterCard International, September 2003.
4. The Aviation and Transportation Security Act, 2001.
5. The Electronic Signatures Act, 2002.
6. The Enhanced Border Security and Visa Entry Reform Act, 2002.
7. The Government Information Security Reform Act (GISRA), 1999.
8. The Homeland Security Act. 2002.
9. Allen, Catherine, "Smart Cards Part of U.S. Effort in Move to ElectroniBanking", Smart Card Technology International: The Global Journal of Advanced Card Technology, ed. Robin Townsend, London: Global Projects Group, 1995

Electronic- Based Resources:

http://www.smartcardalliance.org
http://csrc.nist.gov/pki/
http://www.nacha.org
http://www.ctst.com
http://www.biometrics.org

http://www.gsa.gov/aces