دانشگاه آزاد اسلامی

واحد تهران غرب

گروه کامپیوتر

پایان نامه کارشناسی

عنوان :

کارت‌های هوشمند

استاد راهنما :

دکتر سید نوراله واله

نگارش :

صبا سخاییان‌حاجی‌محمدی

سال تحصیلی:

بهار ۹۴

تشکر و قدردانی

خدای را بسی شاکرم که از روی کرم، پدر و مادری فداکار نسبیم ساخته تا در سایه درخت پربار وجودشان بیاسایم و از ریشه آنها شاخ و برگ گیرم و از سایه وجودشان در راه کسب علم و دانش تلاش نمایم. والدینی که بودنشان تاج افتخاری است بر سرم و نامشان دلیلی است بر بودنم، چرا که این دو وجود، پس از پروردگار، مایه هستی ام بوده اند دستم را گرفتند و راه رفتن را در این وادی زندگی پر از فراز و نشیب آموختند. آموزگارانی که برایم زندگی، بودن و انسان بودن را معنا کردند.

تقدیم به وجود با ارزشتان

چکیده

از حدود چهار دهه قبل، اولین کارت‌های هوشمند به بازار عرضه شدند و به دلیل کاربردهای گسترده آنها با سرعت فزاینده ای در کشورهای مختلف مورد استفاده قرار گرفتند. یک کارت هوشمند عبارت است از جسم فیزیکی کارت که یک تراشه رایانه‌ای برروی آن نصب شده باشد. ظرفیت حافظه این کارت‌ها بین ۱ الی ٦٤ کیلو بایت قابل تغییر است. از طرفی، قابلیت ذخیره سازی و پردازش اطلاعات و نیز، قابلیت بالای مراقبت از اطلاعات ذخیره شده، کاربرد این کارت ها را به کلیه عرصه‌های زندگی انسان گسترش داده است. در این پروژه ضمن معرفی کارت‌های هوشمند و اشاره ای به تاریخچه ظهور و رشد آنها، به فناوری انواع کارت های هوشمند پرداخته شده و پس از برشمردن مزایای استفاده از این کارت‌ها، به کاربردهای کارت در پنج حوزه مختلف، از جمله: حمل و نقل؛ گردشگری؛ فرهنگی – رفاهی؛ پرداخت های روزمره شهروندان و خدمات نیروی انسانی سازمان‌ها توجه شده است.

فهرست

فهرست تصاویر

مقدمه

امروزه ، بشر به این حقیقت دست یافته است که نقل و انتقالات فیزیکی، زمان‌بر، پرهزینه ومحدودکننده‌است و برای آنکه بتواند این مشکل را رفع کند، از ابزارهای مختلفی استفاده کرده‌است. اما وسیله‌ای که بیش از وسایل دیگر، مورداستفاده قرارگرفته وتاکنون بسیاری از مشکلات را حل کرده‌است و از طرفی محدودیت‌های کمتری نیز دارد، انتقال اطلاعات ازطریق تکنولوژی‌های ارتباطی است.

این انتقال، علاوه بر آنکه باعث پیشرفت فعالیت‌ها می‌گردد، محدودیت‌های انتقال فیزیکی را نداشته و حتی در مواردی بهتر ازآن عمل می‌کند.

به عنوان مثال ، در انتقال فیزیکی، امکان بروز خطا، دوباره کاری و... به وفور مشاهده می‌شود درحالی که در انتقال اطلاعات از طریق تکنولوژی ، این موارد به حداقل می‌رسند. انتقال اطلاعات نیازمند یک تکنولوژی است که در جهان به عنوان تکنولوژی اطلاعات شناخته می‌شود.

بهره‌گیری از تکنولوژی و فناوری کارت، به عنوان یکی از دستاوردهای نوین بشری، تحولی عظیم در حوزه‌ی سیستم های کاربری و انتقالی اطلاعات روزمره انسان‌ها ایجاد کرده است و بشر با در دست داشتن این فناوری در زمان و هزینه ی خود صرفه جویی کرده است. دو بحث مهم امنیت و همراه بودن ،از ویژگی‌های برجسته‌ای است که باعث ظهور انواع کارت‌های مختلف شده است.

امروزه روند رو به رشد استفاده از کارت‌ها و آن هم کارت‌هایی با عنوان هوشمند در سطح دنیا و در بیشتر زمینه‌ها قابل مشاهده‌است. به عنوان مثال در بانک‌ها، مراکز مخابراتی، سازمان‌های دولتی، مراکز بهداشتی ، مراکز تفریحی و... . ازنمونه‌های دیگر آن می توان : کارت تلفن، کارت سوخت، کارت‌های سیستم بانکی کشور، کارت رانندگان، کارت بیماری‌های خاص و... را نام برد.

در حال حاضر بیشتر مراکزی که جهت ارائه خدمات به کاربران و یا مشتریان خود از کارت استفاده می‌کنند، در فکر بالابردن فناوری کارت های خود برای بهره‌گیری از مطمئن‌ترین، امن‌ترین و در عین حال مقرون به صرفه‌ترین فناوری هستند. این موضوع بویژه در ایران حائز اهمیت است، چرا که ایران در وضعیتی است که اگر از فواید این تکنولوژی بهره نبرد قطعا از کشورهای مختلف عقب خواهد افتاد.

فصل اول

اهداف و تاریخچه کارت‌های هوشمند

هدف

امروز کارت‌های هوشمند در زندگی بشر نقش مهمی را بدست آورده‌اند که چشم پوشی از کاربردهای فراوان آن غیر ممکن است، هدف از این پایان نامه آشنایی افراد با تاریخچه کارت‌های هوشمند از آغاز اختراع تاکنون است و در ادامه به انواع کارت‌های هوشمند اشاره می‌شود و نحوه تولید و پیاده سازی سامانه های هوشمند در بستر انواع مختلف کارت‌های هوشمند بررسی خواهد شد. هدف اصلی آشنایی بیشتر افراد با فناوری روز دنیا، یعنی هوشمندسازی کارت‌ها می‌باشد.

تاریخچه کارت‌های هوشمند

براساس گزارش‌های منتشر شده، اولین کارت هوشمند حاوی یک ریزپردازنده، در سال ۱۹٦۷ میلادی توسط دو مهندس علوم موشکی آلمانی با نام‌های "هلموت گروتروپ" و همکارش "یورگن دتهلوف" ابداع شد.

در سال ۱۹۷۰ یک دکتر ژاپنی بنام "کونیتاکا آریمورای" مفهوم کلی کارت هوشمند را برای اولین بار به طور انحصاری به ثبت رسانید. اما اختراع کارت هوشمندی که حاوی یک ریزپردازنده باشد، منتشر نشد تا اینکه یک روزنامه نگار فرانسوی با نام " رولاند مورنوی" در سال ۱۹۷٤ میلادی، اختراع کارت IC را در فرانسه ثبت کرد و بعدها این نوع کارت IC به نام "کارت هوشمند" معروف گردید.

در سال ۱۹۷۷ شرکت‌های Bull CP8، SGS Thomson، Schlumberger در این زمینه به فعالیت پرداختند و شروع به ساخت کارت IC کردند. کمپانی موتورولا، در سال ۱۹۷۹ اولین تراشه ریزکنترلر ایمن را برای سیستم بانکی فرانسه ساخت. در سال ۱۹۸۲ استفاده از کارت‌های تلفن عمومی در کشور فرانسه به طور آزمایشی آغاز شد و در سال ۱۹۸٤ نیز آزمایش میدانی کارت‌های خودپرداز در فرانسه با موفقیت روبرو شد. در سال ۱۹۸٦ ، ۱٤,۰۰۰ کارت Bull CP8 بین مشتریان بانک‌های ویرجینیا و مریلند توزیع شد و ۵۰,۰۰۰ کارت کاسیو بین مشتریان بانکهای Palm Beach و Mall توزیع گشت و در این میان اولین

استاندارد برای کارت هوشمند با عنوان (ایزو-۷۸۱۱٦/۱) مطرح شد. در سال ۱۹۸۷ اولین پروژه ی گسترده ی کارت های هوشمند توسط وزارت کشور ایالات متحده آمریکا پیاده سازی شد. پنج سال بعد در سال ۱۹۹۲ ، در کشور دانمارک اولین پروژه کارت‌های پیش پرداخت کلید خورد. پس از دانمارک ، در سال ۱۹۹۳ در شهر رن کشور فرانسه اولین آزمایش میدانی کارت‌های چند منظوره آغاز شد و کارت‌های هوشمند بانکی نیز فعال سازی شدند.

در سال ۱۹۹٤ استانداردی مشترک با نام EMV برای کارت‌های بانکی به وسیله ی انجمن ملی پرداخت کشورهای اروپایی و شرکت‌های Europay ، MasterCard و Visa تدوین گشت و توزیع ۸۰ میلیون کارت با تراشه سریالی در قالب کارت سلامت شهروندی در اختیار مردم کشور آلمان قرار گرفت. این استانداردسازی باعث شد تا امروزه کارت‌های تولید شده توسط سازنده‌های مختلف، به راحتی از طریق سیستم‌های مختلف کارت‌خوان به تبادل و جابجایی اطلاعات بپردازند. در سال ۱۹۹٦ مشترکین تلفن‌های همراه که از کارت‌های هوشمند برای برقراری تماس استفاده می‌کردند به بیش از ۳ میلیون نفر رسید و همچنین توزیع کارت‌های پیش پرداخت در شهر المپیک کشور آتلانتا آغاز گشت، در این سال کارت‌های جاوا با پشتیبانی شرکت قدرتمند Visa و MultOS تحت حمایت شرکت MasterCard توسعه یافتند.

در سال ۱۹۹۸ شرکت مایکروسافت سیستم عاملی مناسب برای کارت‌های هوشمند معرفی کرد و همچنین ۵۰ میلیون کارت هوشمند سلامت در کشور فرانسه توزیع گشت. یک سال بعد کمپانی GemPlus به رکورد استفاده بیش از ۵۰ میلیون سیم‌کارت در سطح جهانی دست یافت.

در سال ۲۰۰۰ میلادی کارت‌های هوشمند غیر تماسی خودرو توسط AutoSmart عرضه گشت که این کارت‌ها علاوه بر نگهداری سابقه تعمیرات اتومبیل ، کاربرد ضد سرقت نیز دارند. سال ۲۰۰۲ کارت های JCB در کنار ترمینال های Hypercom قابلیت امنیتی بیشتری را در اختیار داشت، عرضه شد.

در سال ۲۰۰۳ یک دانشجوی ۱۹ ساله هنگ کنگی کارت‌های هوشمند ماهواره ای را رمزگشایی کرد و آن را در سطح اینترنت پخش کرد که منجر به دستگیری وی شد. در سال ۲۰۰٦ کارت‌های هوشمند به مصارف وزارت دفاع و خارجه ایالات متحده آمریکا رسید و در سال ۲۰۰۷ کارت‌های هوشمند ٦٤ کیلوبایتی که قادر به ذخیره ۲۷ صفحه از پرونده پزشکی را داشت تولید شدند. در سال ۲۰۰۸ شرکت های GemPlus

وAxalto با یکدیگر ادغام شدند و شرکت Gematlo را تشکیل دادند که امروزه از پیشگامان فناوری کارت‌های هوشمند می‌باشد. در سال ۲۰۰۹ بیش از ۵,۲ میلیارد کارت هوشمند براساس حافظه و میکروکنترلر در کاربردهایی مانند سیم‌کارت ، سرویس‌های پرداخت و بانکداری، شناسایی دولتی و معاملات در سراسر جهان به فروش رفت.

بررسی‌های سالانه نشان داده است که یک میلیارد و نیم کارت پرداخت هوشمند در سراسر جهان مورد استفاده قرار می‌گیرد . تنها در ایالات متحده آمریکا حدود ۱۸۵ میلیون کارت قدیمی تغییر شکل داده و به کارت‌های هوشمند تراشه دار تبدیل شده است. این رقم در سال ۲۰۱۳ حدود ۳۰ میلیون کارت بود.

دولت فدرال آمریکا از این تغییر حمایت کرده است و در سال ۲۰۱٤ فرمان اجرائی مربوط به استفاده از تکنولوژی تراشه و پین را صادر کرد.

امروز کارت‌های هوشمند در سراسر جهان با مصارف گوناگون، گاه به صورت تک منظوره و گاه به صورت چند منظوره وجود دارد که از کاربردهای اساسی این نوع کارت‌ها میتوان به کارت‌های اعتباری بانکی، کارت سلامت، کارت سوخت، کارت ملی و .... اشاره کرد.

روش کار و تحقیق

کارت هوشمند معمولا کارتی از جنس PVC با ابعادی در حدود ۵/۵ در ۸/۵ سانتی‌متر است که بر روی آن یا در بین لایه‌های آن، تراشه‌های حافظه و ریزپردازنده برای ذخیره‌سازی داده‌ها و پردازش آنها قرارداده شده است. یک کارت هوشمند کامپیوتر کوچکی است که بر روی یک کارت پلاستیکی نصب شده است. قرار دادن یک تراشه در کارت به جای نوار مغناطیسی، آن را تبدیل به یک کارت هوشمند با کاربردهای گوناگون می‌نماید. این کارت‌ها به دلیل دارا بودن تراشه، قابلیت کنترل عملکرد را داشته و علاوه بر نگهداری اطلاعات شخصی و تجاری کاربر، امکان پردازش را نیز فراهم می‌نماید.

مثلا در یک شرکت که دارای شعبه‌ها، واحدها و بخش‌های بسیاری است و کارکنان در آن به محدوده‌ها و مکان‌های مرتبط خود اجازه دسترسی دارند. همچنین کارکنان به شبکه و سرورها برای انجام فعالیت‌های خود و کارهای مختلف دسترسی خواهند داشت از قبیل ارسال نامه الکترونیکی، دسترسی به اینترنت، دسترسی به اطلاعات و بانک‌های اطلاعاتی. بنابراین کلیدها، کلمه‌های عبور و کدهای امنیتی مختلفی را کارکنان باید در اختیار داشته باشند و برای استفاده از رستوران شرکت و مکان‌های رفاهی باید همیشه پول همراه خود داشته باشند. می‌توان با استفاده از کارت‌های هوشمند چند منظوره پروسسوری (که سیستم‌عامل جاوا در آن اجازه این عملیات چندگانه را می‌دهد) کلیه این عملیات امنیتی و اعتباری را مدیریت نمود. بنابراین شرکت باید یک سیستم مدیریت و گواهی دسترسی(Certificate Authority) محلی فراهم نماید. شکل زیر یک ساختار ساده PKI را نشان می‌دهد.

(شکل شماره ۱ – ساختار ساده یک PKI)

به این منظور با بررسی مقالات متعدد به شناسایی کارت هوشمند و نحوه ی عملکرد آن در این پایان نامه می‌پردازیم.

فصل دوم

کارت هوشمند

کارت هوشمند

کارت هوشمند بطور معمول یک نوع کارت پلاستیکی دارای یک تراشه جاسازی شده می‌باشد. یک نوع حافظه یا ریزپردازنده که داده‌ها را ذخیره و منتقل می‌کند. این‌ها معمولاً حاوی اعتبار یا اطلاعات و گاهی هردو می‌باشند و در تراشه کارت، ذخیره و پردازش می‌شود. داده‌های درون کارت از طریق یک کارت‌خوان که بخشی از یک سیستم محاسباتی است خوانده می‌شود. سازمان‌هایی با کارت‌های هوشمند ارتقاء یافته‌اند، از جمله بهداشت و درمان، بانکداری، سرگرمی و حمل و نقل، که امروزه از برنامه‌های کاربردی مختلف بسیاری استفاده می‌کنند. همه برنامه‌های کاربردی می‌توانند از ویژگی‌های افزوده شده و ایمنی که کارت‌های هوشمند فراهم می‌سازند بهره مند شوند.

بر طبق یورو اسمارت، ارسال کارت هوشمند در سال ۲۰۱۰ با تعداد ۵٤۵۵ میلیارد کارت ۱۰٪ رشد در سرتاسر جهان داشت. بازاری که بطور سنتی بوسیله تکنولوژی دستگاه کارت خوان مانند بارکد و نوار مغناطیسی عمل می‌کرده است اکنون به کارت هوشمند تبدیل شده، بطوریکه در بازدید سالیانه، در سرمایه گذاری برای هر صادرکننده کارت بعنوان کلیدی، محاسبه می‌شود.

برنامه کاربردی

برای نخستین بار کارت‌های هوشمند، حدود سی سال پیش در اروپا به عنوان ابزاری برای ذخیره سازی اعتبار، در تلفن‌های همگانی به منظور کاهش سرقت آغاز بکار کرد و بدین ترتیب کارت‌های هوشمند و دیگر کارت‌های مبتنی بر تراشه پیشرفت کردند. مردم راههای جدیدی برای استفاده از آنها پیدا کردند از جمله کارت شارژ برای خریدهای اعتباری و برای نگهداری سوابق به جای استفاده از اسکناس.

درایالات متحده آمریکا ، مصرف کنندگان، از کارت‌های تراشه در بسیاری از کارها استفاده می کنند از جمله کتابفروشی‌ها، خرید مواد غذایی و سینما رفتن، و به نوعی در زندگی روزمره بطور ثابت جای گرفته است. در چند ایالت آمریکا برنامه‌های کارت تراشه در نرم افزارهای دولت اعم از بخش وسایل نقلیه موتوری تا

انتقال نیروی الکتریکی مورد استفاده قرار می‌گیرد. بسیاری از صنایع، کارت‌های هوشمند را در محصولات خود، از جمله تلفن همراه دیجیتال جی اس ام و همچنین برای رمزگشایی کدهای تلویزیون‌های ماهواره‌ای بکار گرفته‌اند.

چرا کارت هوشمند ؟

کارت‌های هوشمند امنیت هر نوع معامله را بهبود می‌بخشند. امکان دستکاری کاربر در ذخیره‌سازی و شناسایی حساب در این کارتها وجود ندارد. ثابت شده است که سیستم‌های کارت هوشمند قابل اعتمادتر از دیگر کارتهای ماشین‌خوان، نظیر نوارمغناطیسی و بارکد هستند. با مطالعه بسیار، ثابت شد که دوام کارت‌ها و دستگاه‌های کارت‌خوان بیشتر از هزینه نگهداری سیستم آنها است. کارت‌های هوشمند نیز اجزای حیاتی سیستم‌های امنیتی برای تبادل داده‌ها را، تقریباً در سرتاسر هر نوع شبکه‌ای را فراهم می‌کند. آنها در برابر طیف گسترده‌ای از تهدیدات امنیتی، اعم از بی‌دقتی کاربر در ذخیره‌سازی کلمه عبور تا هک‌های پیچیده سیستم محافظت می‌کنند. هزینه راه اندازی رمز عبور برای یک سازمان یا شرکت بسیار بالا است، بنابراین ساخت کارت‌های هوشمند یک راه مقرون به صرفه در این محیط‌ها است. کارت‌های چند منظوره نیز می‌توانند برای دسترسی به شبکه و ذخیره اعتبار و داده‌های دیگر مورد استفاده قرار گیرند. در سراسر جهان مردم برای کارهای روزمره از کارت‌های هوشمند استفاده می کنند که عبارتند از :

سیم‌کارت و مخابرات

معروفترین نرم‌افزار تکنولوژی کارت هوشمند، مدل هویت مشترکین (SIM) است که برای همه سیستم‌های تلفن که تحت استاندارد سیستم جهانی ارتباطات (GSM) هستند ضروری است. هر تلفن با بهره‌گیری از شناسه منحصر بفرد در سیم‌کارت ذخیره شده تا حقوق و امتیازات هر کاربر در شبکه‌های مختلف حفظ شود.

این حالت نشان می دهد که بیش از نیمی از تمام کارت‌های هوشمند در هر سال مصرف می شوند. از مدل شناسایی جهانی مشترکین (USIM) نیز بعنوان پل هویتی برای انتقال بین اپراتورهای شبکه UTMS، GSM و 3G استفاده می شود.

وفاداری و اعتبار موجودی

یکی دیگر از استفاده‌های کارت هوشمند، اعتبار موجودی است، مخصوصاً برنامه‌های وفاداری است که مشتریان را پیدا کرده و آنها را به استفاده مجدد تشویق می کند. اعتبار موجودی راحتر و امن تر از پول نقد است. برای صادر کنندگان کارت ، مبالغ هزینه نشده شناور و باقیمانده مبالغی که تا بحال مورد استفاده قرار نگرفته قابل تشخیص است. برای خرده فروشان زنجیره ای که برنامه وفاداری را در بسیاری از کسب و کارهای مختلف و سیستم POS استفاده می کنند، کارت هوشمند می تواند تمام داده‌ها را بصورت مرکزی پیگیری و مشخص کند. برای این منظور برنامه‌های کاربردی متعددی هستند مانند حمل ونقل، پارکینگ، لباسشویی، بازی، خرده فروشی و سرگرمی.

ایمن سازی مضمون دیجیتالی و دارایی های مادی

کارت هوشمند علاوه بر اطلاعات امنیتی، با محدود کردن دسترسی به حساب دیگران و تنها امکان دسترسی توسط افرادی که دارای مجوز هستند می تواند امنیت بیشتر خدمات و تجهیزات را تضمین کند.

اطلاعات و سرگرمی از طریق ماهواره و تلویزیون های کابلی به دستگاه پخش DVR ، جعبه کابل یا کابل فعال PC ارسال می شود. تحویل خانگی خدمات رمز دار و رمز گشایی از طریق کارت هوشمند در دسترس هر مشترک قرار می گیرد. سیستم پخش ویدئویی دیجیتال، کارتهای هوشمند را بعنوان کلید الکتریکی ایمنی پذیرفته است.

از کارتهای هوشمند نیز می توان به عنوان کلیدهای تنظیم تجهیزات حساس آزمایشگاهی و نسخه پیچی برای داروها، ابزار، کارتهای کتابخانه، تجهیزات باشگاه سلامت و غیره استفاده کرد. در برخی از محیط ها،

کارت هوشمند، SD را توانا می‌کند و کارتهای میکرو SD مضمون دیجیتال را هنگام انتقال به دستگاه موبایل یا تلفن محافظت می کنند.

تجارت الکترونیک

کارت‌های هوشمند کار ذخیره امن اطلاعات و نقدینگی را برای خرید مصرف کنندگان ساده می کنند. فوائدی که به مصرف کنندگان ارائه می کند به قرار زیر است :

- ✓ کارت می تواند شرح حساب را در برداشته باشد، تنظیمات اطلاعات اعتباری و خرید که به جای پر کردن فرم با کلیک یک ماوس قابل دسترسی است.
- ✓ کارت‌ها می‌توانند هزینه‌ها را با محدودیت‌های اتوماتیکی و گزارش‌دهی، کنترل و مدیریت کنند.
- ✓ برنامه‌های وفاداری اینترنتی را می‌توانند در بین فروشندگان با سیستم‌های مختلف POS ایجاد کند و بعنوان یک بایگانی سپرده‌گذاری ایمن مرکزی ، برای امتیازها و پاداش‌ها عمل کند .
- ✓ پرداخت میکرو: پرداخت، هزینه‌های جزئی بدون حق الزحمه معامله با کارت‌های اعتباری، یا برای مقادیر بسیار کم پول نقد، مانند هزینه های چاپ مجدد را پرداخت می‌کند.

کارتهای هوشمند صادر شده توسط بانک

در سرتاسر جهان، بانک‌هایی که بر کارت‌های هوشمند اعتباری (ویزا ، مسترکارت ، دیسکاور و آمریکن اکسپرس) نظارت دارند، میلیون‌ها کارت هوشمند تحت استاندارد EMV (یوروپی، مسترکارت و ویزا) به گردش در آورده‌اند. این کارت‌ها اغلب به تراشه یا پین کارت منتسب هستند. این نوع کارت برای صدور بانکی در بسیاری از کشورها به جز ایالات متحده به صورت غیر رسمی صادر می‌شود. کانادا به تازگی جابجایی را با استفاده از کارتهای EMV شروع کرده است، از بین کشورهای آمریکای شمالی، آمریکا تنها کشوری است که این تغییر را نپذیرفته است. این مسئله باعث شده جعل هر دو نوع کارت اعتباری و کارت

بدهی افزایش یابد. ثابت شده است که کارت‌های هوشمند معاملات را با نظم و قاعده تضمین می‌کنند. آنقدر که استاندارد EMV به یک اصل قانونی تبدیل شده است.

همانگونه که بانک‌ها، وارد بازار تازه رقابتی سرمایه‌گذاری باز دلالی می شوند، تامین امنیت معاملات از طریق کارت‌های هوشمند افزایش می‌یابد که به این مفهوم است :

- ✓ کارت هوشمند با ایجاد ایمنی باعث افزایش اعتماد می شود. دو فاکتور اعتبار حفاظت داده‌ها و ارزش را درسراسر اینترنت تضمین می‌کنند. تهدیدهایی مانند " مردی در راه" و " اسب تروا " که بعنوان نام کاربر استفاده می شود و رمز عبور حذف می شود.
- ✓ این کار باعث بهبود خدمات مشتریان می‌شود. مشتریان می‌توانند بصورت شبانه‌روزی ازکارت‌های هوشمند ایمن، برای انتقال سریع الکترونیکی در سرتاسر اینترنت استفاده کنند.
- ✓ هزینه‌ها کاهش می‌یابد. معاملاتی که درحالت عادی نیاز به اتلاف وقت یک کارمند بانک و کارهای کاغذی دارد با روش الکترونیکی با کارت هوشمند می توانند انجام یابند.

بهداشت و درمان انفورماتیک

وسعت داده‌های سلامت برای مراقبت کافی بیماران وحریم خصوصی امنیتی آنها چالش‌های جدیدی را مطرح می کند. کارت‌های هوشمند هر دو نوع این چالش‌ها را همراه با ذخیره سازی ایمن موبایل و توزیع اطلاعات بیمار اعم از داده‌های اضطراری و وضعیت مزایا را اداره می‌کنند. بسیاری از کشورهای سوسیالیستی کارت‌های هوشمند را در شبکه بهداشتی خود به عنوان وسیله حمل پرونده سلامت الکترونیکی قابل بازیافت سریع پذیرفته‌اند. مزایای کارت‌های هوشمند در حوزه سلامت و بهداشت شامل موارد زیر می‌باشند:

- ✓ شناسایی دقیق و سریع بیماران، اصلاح درمان.
- ✓ کاهش تقلب از طریق احراز هویت ارائه دهنده، ویزیت بیماران و واجد شرایط بیمه بودن آنها.
- ✓ یک راه مناسب برای حمل داده‌ها بین سیستم و یا به سایت‌های بدون سیستم.

- ✓ کاهش هزینه‌های نگهداری سابقه.

تعبیه کنترل در دستگاه پزشکی

سالیان بسیاری است که کنترل کننده‌ها در انواع مختلف ماشین‌آلات قرار داده شده‌اند تا ناظر برکیفیت و دقت عملکرد آنها باشند. در بهداشت و سلامت، کارت‌های هوشمند جاسازی شده در وسایل مراقبتی همچون دستگاه دیالیز، تجزیه و تحلیل خون و تجهیزات عمل لیزر چشم بهترین و ایمن‌ترین خدمات را تضمین می‌کنند.

تشکیلات اقتصادی و امنیت شبکه

ویندوز مایکروسافت، سیستم‌های سان مایکرو (یک شرکت تابعه از شرکت اوراکل) و همه نسخه‌های جدید لینوکس یک نرم افزار به شبکه وصل کرده‌اند که کارت‌های هوشمند را جایگزین نام کاربری و کلمه عبور می‌کند. مایکروسافت یک پلتفرم اعتباری کامل در اطراف اسکارد DLL و تامین‌کننده خدمات رمزنگاری CSP ساخته است. شرکت‌ها با این درک که افزایش ایمنی زیر ساخت کلید عمومی PKI است و به بشدت مورد نیاز کارکنان است، کارت‌های هوشمند به عنوان یک نشان مشخص استاندارد جدید است. تجارت اینترنتی و شبکه‌های خصوصی مجازی با استفاده از کارت هوشمند افزایش یافته‌است. کاربران می‌توانند اعتبار کسب کنند و براساس امتیازات از پیش تعیین شده مجاز به دسترسی به اطلاعات خاصی باشند. دامنه برنامه‌های کاربردی از ایمیل ایمن تا تجارت الکترونیکی کشیده می‌شود.

دسترسی فیزیکی

هر نوع موسسه تجاری و دانشگاه‌ها برای کارکنان و دانشجویان خود به کارت‌های شناسایی ساده‌ای نیاز دارند. اکثر این افراد اجازه دسترسی به داده‌ها، تجهیزات و بخش‌های خاصی دارند. کارت‌های چند کاره

هوشمند میکروپروسسوری ترکیبی از هویت و مزیت دسترسی را دارند و همچنین می‌توانند اعتبار را ذخیره کنند تا در بسیاری از مکان‌ها مانند کافه تریا و فروشگاه‌ها مورد استفاده قرار گیرند. بسیاری از هتل‌ها هم کارت‌خوان نوع ISO ٧٨١٦ را پذیرفته اند تا بدین طریق امنیت کارمندان، اتاق‌ها و تجهیزات را تامین کنند.

در حال حاضر دولت ایالات متحده آمریکا و بسیاری از شرکت‌ها یک دستگاه کارت‌خوان غیرتماسی را بعنوان نقطه دسترسی به امکانات خود بکار گرفته‌اند. برخی از شرکت‌های یک جزء بیومتریک نیز به این کارت‌های اعتباری افزوده‌اند. سیستم‌های قدیمی‌تر به عنوان محافظت مدخل، یک سیستم مجاور به کارت را نصب کرده‌اند لیکن بهمان اندازه که نیازهای امنیتی افزایش داشته هزینه سیستم استاندارد ISO ١٤٤٣ کاهش یافته است، جهان بسرعت این استاندارد جدید را پذیرفته است. این تغییر بازار بخشی از دستور تایید هویت شخصی (PIV) از طرف دولت ایالات متحده است. یک هماهنگی قوی از طرف تامین کنندگان و فروشندگان برای این استاندارد وجود دارد.

فصل سوم

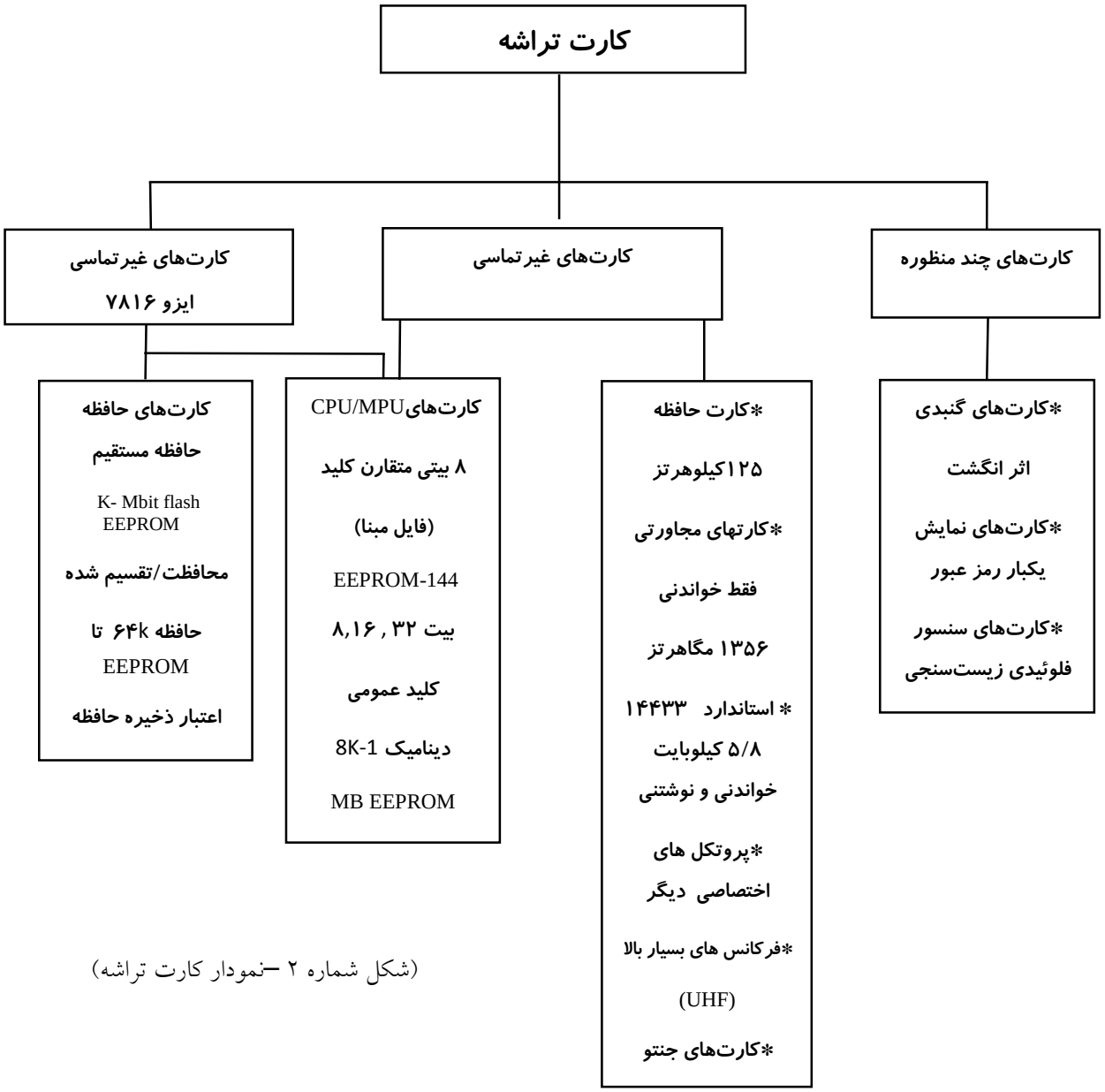
انواع و استانداردهای کارت‌های هوشمند

انواع کارت‌های هوشمند

کارت‌های هوشمند با توجه به موارد زیر اینگونه تعریف می‌شوند :

۱) نحوه خوانده و نوشته شدن اطلاعات کارت

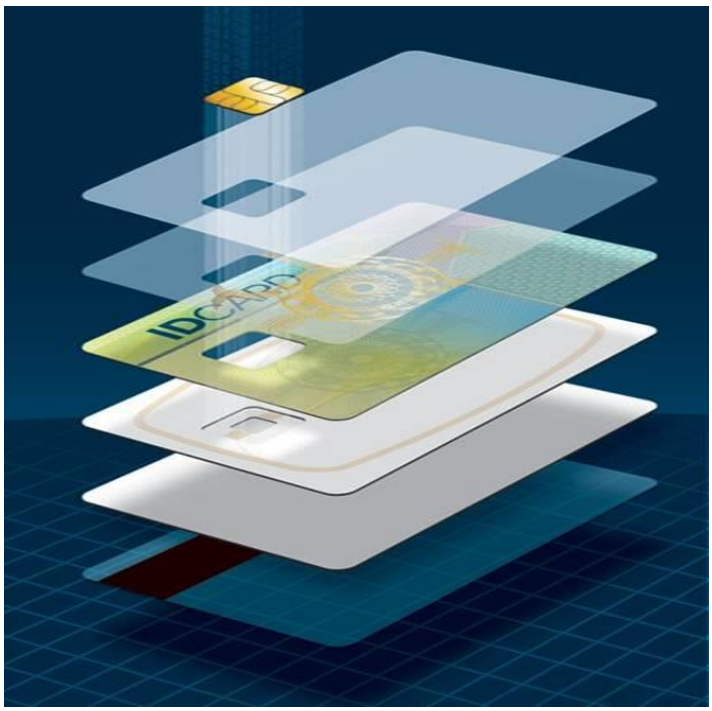
۲) نوع تراشه درون کارت و قابلیت های آن. از وقتیکه که سیستم طراحی می شود. طیف گسترده ای از گزینه های انتخابی وجود دارد.



(شکل شماره ۲ –نمودار کارت تراشه)

ساختمان کارت

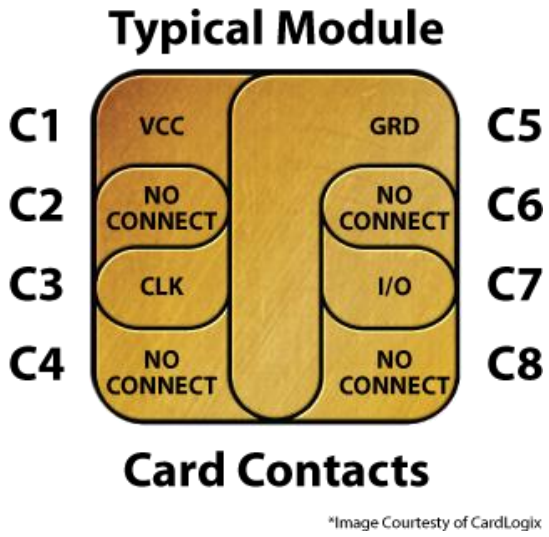
اکثر کارت‌های تراشه از لایه‌هایی با مواد مختلف ساخته شده‌اند، یا لایه‌هایی که بطور صحیح به هم وصل شده و باعث می‌شود به کارت دوام و قابلیت خاصی بدهد. امروزه کارت معمولی از ماده PVC، پلی استر یا پلی کرنت ساخته می شود. ابتدا لایه‌های کارت چاپ می شوند سپس بصورت ورقه ورقه با فشار زیاد رویهم قرار می‌گیرند. مرحله بعدی بلنکینگ و برش زنی است. این کار پس از اضافه کردن یک تراشه و بعد از افزودن داده‌ها به کارت است. بطور کلی، ممکن است ۳۰ مرحله برای ساخت یک کارت وجود داشته باشد. همه اجزاء، شامل نرم افزار و پلاستیکها، احتمالاً تعداد ۱۲ آیتم جداگانه، همه در یک پکیج واحد قرار می‌گیرند که برای کاربر مانند یک وسیله ساده بنظر می رسد.



(شکل شماره ۳ – ساختار کارت هوشمند)

کارت‌های تماسی

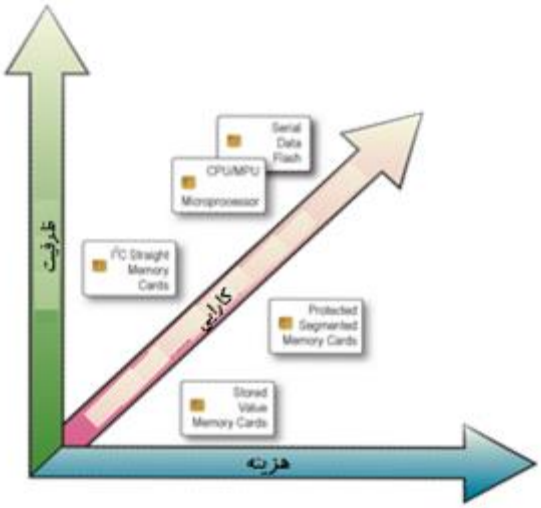
این نوع کارت‌ها، رایج ترین نوع کارت‌های هوشمند هستند . تماس‌های الکترونیکی در بیرون کارت متصل به کارت‌خوان قرار دارند، وقتی کارت وارد دستگاه کارت خوان می‌شود. این اتصال دهنده به تراشه محصور شده در کارت پیوند دارد.



(شکل شماره ٤ – تراشه کارت تماسی)

افزایش سطح قدرت پردازش،افزایش انعطاف پذیری و افزایش حافظه باعث افزایش هزینه می‌شود. معمولاً کارت تابع تک منظوره مقرون به صرفه ترین راه حل است. نوع درست کارت برای برنامه کاربردی باید انتخاب شود. سطح ایمنی مورد نیاز، ارزیابی هزینه در مقابل عملکرد باید تعیین شود و در پیوند با هزینه عناصر سخت افزاری در گردش، کار معمولی مشخص گردد.

همه این متغیرها باید در مقابل چرخه دوام کارت اندازه گیری شوند. بطور متوسط کارت‌ها عموماً ۱۰ تا ۱۵ در صد مجموع هزینه سیستم با پایه‌ریزی، بیمه، نرم افزار، کارت‌خوان‌ها، آموزش و تبلیغات را تشکیل می‌دهد. چارت ذیل برخی از قوانین کلی را نشان می دهد :



(شکل شماره ۵ – نمودار قوانین کارت هوشمند)

کارت‌های حافظه

کارت‌های حافظه، توانایی مدیریت فایل و پردازش داده‌ها را ندارند. همه کارت‌های حافظه از طریق قرارداد از پیش تعیین شده با کارت‌خوان‌ها ارتباط برقرار می‌کنند. در همه کارت‌های حافظه یک نشانی ثابت روی کارت خوانده و نوشته می‌شود. سه نوع اصلی کارت‌های حافظه وجود دارد: راست، محافظتی، ارزش ذخیره شده. قبل از طراحی این کارت‌ها برای یک سیستم گیرنده، صادرکننده باید بررسی کند که آیا کارت‌خوان‌ها و یا ترمینال‌ها، پروتکل ارتباط تراشه را ساپورت می‌کنند. اکثر کارت‌های بدون تماس اصطلاحاً در حافظه حفاظتی یا کارت حافظه بخش‌بندی شده، مختلف هستند.

کارت‌های حافظه راست

این کارت‌ها فقط داده‌ها را ذخیره می‌کنند و توانایی پردازش داده‌ها را ندارد. اغلب با I۲C یا سریال فلش نیمه هادی، ساخته می‌شود. این کارت‌ها بطور سنتی کمترین هزینه را در هر بیت حافظه کاربر دارند. البته

اکنون با مقادیر بزرگتر از پردازنده درحال ساخت برای بازار GSM تغییر کرده است که باعث استفاده چشمگیری از این نوع دستگاه‌ها شده است. آنها باید به عنوان فلاپی دیسک در اندازه های مختلف بدون مکانیزم قفل در نظر گرفته شوند.

این کارت‌ها نمی‌توانند خود را به کارت‌خوان شناسایی کنند، بنابراین سیستم میزبان باید بداند که چه نوع کارت به دستگاه کارت‌خوان وارد شده است. این کارت‌ها بسادگی المثنی می‌شوند و از طریق شناسه کارت نمی‌توانند ردیابی شوند.

کارت‌های حافظه حفاظتی و بخش‌بندی شده

این نوع کارت‌های جاسازی شده برای کنترل دسترسی به حافظه کارت ساخته شده‌اند. گاهی به کارت‌های حافظه، کارت‌های هوشمند نیز گفته می شوند، این دستگاه‌ها قادرند برای نوشتن و حفاظت برخی یا همه آرایه‌های حافظه فرستاده شوند. بعضی از این کارت‌ها توانایی پیکربندی را دارند تا دسترسی به خواندن و نوشتن را محدود کنند. معمولاً این کار از طریق رمز عبور و یا سیستم کلیدی انجام می‌شود. کارت‌های حافظه را می‌توان به بخش‌های منطقی به نسبت وظایف تقسیم کرد. این کارت‌ها براحتی قابل کپی کردن نیستند اما احتمالاً می‌توانند توسط هکرها جعل هویت شوند. بطور معمول آنها را می توان با یک شناسه در کارت رد یابی کرد.

کارت حافظه اعتباری

این کارت‌ها مشخصاً به منظور ذخیره اعتبار و یا اجازه ورود طراحی شده اند. کارت‌ها یا یکبار مصرف یا قابلیت شارژ مجدد دارند. اکثر این نوع کارت‌ها دارای اقدامات امنیتی دائمی در طول تولید می‌باشند. این اقدامات شامل کلید رمز و منطق است که وارد کردن رمز دشوار به تراشه، توسط کارخانه صورت میگیرد. آرایه های حافظه این وسیله ها بطریق کاهش پله ای یا شمارنده ها برقرار می‌شوند. برای کارهای دیگر مقدار کمی یا اصلاً حافظه‌ای باقی نمی‌ماند. در برنامه‌های کاربردی ساده مانند کارت تلفن ، تراشه ٦٠ یا

۱۲ سلول حافظه دارد، برای هر یک واحد، یک سلول وجود دارد هر گاه یک واحد تلفن استفاده شود یک سلول حافظه پاک می شود. وقتی همه حافظه استفاده شود کارت بی مصرف می‌شود و دور انداخته می‌شود. در صورتیکه کارت قابلیت شارژ داشته باشد این فرآیند معکوس می شود.

کارت‌های میکروپروسسور چندمنظوره CPU/MPU

این کارت‌ها قابلیت پردازش دینامیکی داده‌ها را بر روی کارت دارند. کارت‌های هوشمند چندمنظوره به کارت‌حافظه اختصاص دارند که در بخش‌های مستقل یا فایل‌هایی که برای کار یا برنامه کاربردی خاصی تعیین شده‌اند در داخل کارت یک تراشه میکروپروسسور یا میکروکنترلر وجود دارد که کار تقسیم حافظه و دسترسی به فایل‌ها را مدیریت می‌کند. این نوع تراشه شبیه به آنهایی که در کامپیوتر شخصی هستند می‌باشد و وقتی در یک کارت هوشمند قرارداده می‌شود، داده‌ها را با ساختار منظم از طریق سیستم اپراتوری (COS) مدیریت می‌کند. بر خلاف سیستم اپراتوری‌های دیگر، این نرم افزار دسترسی به کارت‌حافظه روی کارت کاربر را کنترل می کند. این قابلیت به کارت اجازه می‌دهد تابع چند منظوره و یا برنامه‌های کاربردی مختلف روی کارت قرار گیرند، که از طریق کارت به معاملات فرصت صدور و حفظ تنوع "محصولات" می‌دهد. یک نمونه از این موارد کارت بستانکاری است که در یک محوطه دانشگاه امکان دسترسی را به ساختمان را می‌دهد. کارت‌های چند منظوره با انجام معاملات مدرن و تکنولوژی رمزدار، برای صادرکننده کارت ایجاد بازار محصولات و خدمات سودآور می‌کند. بویژه، این تکنولوژی، ایمنی هویت کاربر را تامین می‌کند و بدون جابجایی کارت‌های پایه بروزرسانی اطلاعات، ساده سازی و تغیرات برنامه ها را مجاز می‌سازند. برای کاربر، کارت چند منظوره به مفهوم سهولت و ایمنی بیشتر و نهایتاً ترکیب کارت‌های چندگانه به تعداد کمتر که برای چند منظور بکار می روند.

پیکربندی تراشه در این طبقه‌بندی متعدد است، از قبیل تراشه هایی که با کلید رمز زیر ساخت عمومی (PKI) همراه با کمک پردازنده محاسباتی یا کارت جاوا و نیز دستگاه بلوک‌های سخت‌افزار کار می‌کند. با یک حساب سرانگشتی هر چه کار بیشتر باشد، هزینه نیز بیشتر می‌شود.

کارت‌های غیر تماسی

کارت‌های هوشمند این مدل با یک فرکانس رادیویی (RFID) بین کارت و کارت‌خوان بدون تعبیه فیزیکی کار می‌کنند درعوض کارت از قسمت خارجی کارت خوان عبور داده و خوانده می‌شود. انواع آنها شامل کارت‌های مجاورتی که بعنوان فقط کارت‌خوان است و یک تکنولوژی برای دسترسی به ساختمان بکار می‌روند. این کارتها با حافظه محدود کار می کنند و در ۱۲۵ MHz ارتباط برقرار می‌کنند. نوع دیگری از کارت محدود UHF Gen ۲ هستند که در ۸٦۰ MHz تا ۹٦۰ MHz راه اندازی می‌شوند.

کارت‌های واقعی خواندنی و نوشتنی غیرتماسی اولین بار در برنامه‌های کاربردی حمل و نقل برای کاهش پله‌ای و اعتبارگذاری مجدد هزینه استفاده می‌شدند، زمانی که ایمنی مسئله‌ای نبود. آنها در ۱۳/٥٦ MHz و با استاندارد ISO ۱٤٤٤۳ ارتباط برقرار می‌کردند در ضمن در اعتبار فروشگاه‌های خرده فروشی، کارت-هایی مانند (کارت ویزا و مستر کارت) بر خلاف کارت‌های هوشمند سنتی توانستند بدون کاهش سود، پردازش معاملات را سرعت بخشند.

خصوصیات متغییرهای ISO ۱٤٤٤۳ شامل A ، B، و C هستند که تراشه‌های نوع اصلی را از جعلی مشخص می‌کنند.

A = NXP
B = (فیلیپس) دیگران
C = فقط تراشه های سونی

بر خلاف کارت‌های میکروپروسسور و فاصله محدود کارت و کارت‌خوان که برای عملیات لازم است کارت‌های هوشمند غیرتماسی شامل محدودیت کارهای نهفته و حافظه کاربر است.

کارت‌های ارتباطی چند وجهی

این کارت‌ها دارای چند روش ارتباطی هستند شامل استاندارد ISO ۷۸۱٦ و استاندارد ISO ۱٤٤٤۳ و UHF Gen ۲ . نحوه ساخت کارت تعیین می‌کند که آیا پیوندی و یا واسط دوتایی هستند. این اصطلاح شامل کارت‌هایی است که نوار مغناطیسی یا بارکد و یا هر دو را دارند.

کارت‌های پیوندی

کارت‌های پیوندی دارای چند تراشه روی یک کارت هستند. این نوع کارت‌ها توسط یک واسطه جداگانه به یکدیگر متصل شده‌اند مانند تراشه MIFARE و آنتن ۷۸۱۶ که همه در یک کارت مشترک هستند.

کارت دوگانه واسطه‌دار

این نوع کارت یک تراشه کنترل کننده ارتباطی دارد. با روش استنتاجی یا مکانیزم برآمدگی قابل انعطاف. تراشه ممکن است توسط یک ارتباط قوی به آنتن متصل یا درونش جا داده شده باشد.

عوامل شکل‌دهی کارت هوشمند

شکل کارتها اغلب بافرم ۸۰ CR است. کارت‌های بانکی و هویت با مشخصات استاندارد ISO ۷۸۱۰ تهیه می شوند. اما این تنها عامل فرم‌دهی کارت‌هایی که ساخته می‌شوند نیست. در سراسر جهان برش‌های مدل موج‌گیر برای کارت‌ها اختصاص داده شده‌است. رایج‌ترین شکل‌ها سیم کارت‌های اس‌دی و میکرو-اس‌دی که می‌توانند تراشه‌های کارت هوشمند با دوام بکار برده شوند. درایو فلش یواس‌بی رمزی نیز موجود است که قدرت نفوذی مشابه در تکنولوژی کارت با فاکتور متفاوت را دارد.

مدارهای یکپارچه و سیستم عامل کارت

دو نوع اصلی سیستم عامل کارت هوشمند بقرار زیر می باشند:

۱- ساختار فایلهای ثابت

۲- سیستم برنامه کاربردی پویا

مانند انواع سیستم کارت‌های هوشمند، انتخاب یک سیستم عامل، به برنامه در نظر گرفته شده برای کارت بستگی دارد. تفاوت دیگری که می‌توان تعریف کرد قابلیت‌های رمز گذاری سیستم عامل روی تراشه است. انواع رمزگذاری‌ها کلید متقارن و کلید نامتقارن نام دارند (کلیدهای عمومی).

انتخاب تراشه برای این توابع گسترده است و توسط بسیاری از تولیدکنندگان نیمه‌هادی، پشتیبانی می‌شود. آنچه که تراشه یک کارت هوشمند را از دیگر میکروکنترلرها جدا می کند اغلب به عنوان سیلیکون اعتباری نامیده می شود. خود دستگاه طوری طراحی شده تا داده‌ها را بصورت ایمن ذخیره شود تا در مقابل دخالت‌های الکتریکی خارجی یا هک‌شدن مقاومت نماید. این ویژگی ایمنی دارای یک لیست بلند مکانیزم-هایی همچون بدون سوزن آزمایشی، پوشش فلزی حفاظتی مخصوص و طرح‌بندی نامرتب ساختمان دریچه‌های سیلیکون است.

لیست سیلیکون اعتباری نیمه هادی وندور سال ۲۰۱۰ به شرح زیر می باشد :

- Atmel
- EM Systems
- Infineon
- Microchip
- NXP
- Renesas Electronics
- Samsung
- Sharp
- Sony
- ST Microelectronics

بسیاری از ویژگی‌های مورد درخواست کاربران، چیزهایی مانند الگوریتم رمزگذاری خاص است که در معماری مجموع برنامه تراشه‌های سخت افزار و نرم افزار گنجانیده شده است که اغلب می‌تواند در تولید کارت نتیجه داشته باشد. در انتخاب کارت وندور باید دقت داشت که بتواند پروژه را به مرور زمان حمایت کند، نظر به اینکه سیستم عامل کارت فروشنده در بازار دارای نوساناتی است. ابزار و میان‌افزاری که

سیستم‌عامل کارت را حمایت می کنند به همان اندازه که تراشه اهمیت دارد مهم هستند. ابزار پیاده سازی پروژه برای استفاده باید ساده باشد و قدرت بکارگیری سریع پروژه را فراهم کند.

ساختار ثابت فایل سیستم‌عامل کارت

ساختار ثابت فایل سیستم عامل کارت این نوع کارت‌ها را به عنوان یک وسیله ذخیره‌سازی و محاسباتی ایمن تلقی می‌کند. قبل از کار فایل‌ها و دستورات توسط صادرکننده گذاشته می‌شود. این پارامترهای خاص برای یک نوع ساختار ثابت و فعالیت کارت که در آینده نزدیک تغییر نمی‌کنند ایده آل و مقرون به صرفه هستند. بسیاری از برنامه‌های ذخیره اعتبار و بهداشت ایمن از این نوع کارت استفاده می‌کنند. می توان به هزینه کم کارت اعتبار چند منظوره ایمن اشاره کرد. برخلاف برخی مقالات مغرضانه، این سبک کارت را می‌توان با ذخیره مولفه‌های بیومتریک و کارت‌خوان بخوبی بکار برد. در سطح جهانی، این نوع کارت‌های میکروپروسسور رایج‌ترین هستند.

برنامه پویا سیستم عامل کارت

این نوع سیستم عامل، که شامل کارت جاوا و انواع کارت اختصاصی MULTOS هستند سازندگان را قادر می‌سازند تا برنامه‌های کاربردی ایمن روی کارت را بسازند و پس از آزمایش بکار برند. زیرا سیستم عامل و برنامه‌های کاربردی بیشتر جدا هستند بروز رسانی امکان پذیر است.

کارت هوشمند خوان‌ها و ترمینال‌ها

کارت‌خوان‌ها و ترمینال‌ها با کارت‌های هوشمند راه‌اندازی می‌شوند تا اطلاعات کارت، جهت اجرای تراکنش را دریافت کنند. بطور کلی، یک کارت‌خوان با یک PC ارتباط برقرار می‌کند تا آنچه را که مورد

نیاز است، پردازش کند. ترمینال یک دستگاه خودپردازشگر است. کارت‌خوان‌ها و ترمینال‌ها بر روی کارت-های هوشمند کار نوشتن و خواندن را انجام می‌دهند.

اتصال

این نوع کارت‌خوان‌ها به ارتباط فیزیکی نیاز دارند که توسط قرار دادن کارت به درون کارت‌خوان انجام می‌شود. این رایج‌ترین نوع کارت‌خوان برای برنامه های کاربردی همچون ID و کارت‌اعتباری هستند. ارتباط بین کارت‌خوان و کارت اغلب فقط از طریق استاندارد T=۰ ISO ۷۸۱٦ است. این ارتباط مزیت اتصال مستقیم به کارت‌خوان را دارد و از ایمنی بیشتری برخوردار است. مزیت دیگر آن سرعت بالا است. پروتکل PTS نمونه انتخابیISO ۷۸۱٦ با سرعت قابل انتقال تا حدود ۱۱۵ کیلو در ثانیه می‌تواند باشد. این ارتباط می‌تواند داده‌های بیشتری را انتقال دهد بدون افزایش هزینه‌های ضد برخورد و پیامدهای ازکارافتادگی بیسیم که در نتیجه حرکت کارت به داخل و خارج از کارت‌خوان است.

(شکل شماره ٦ – کارتخوان تماسی)

غیرتماسی

این نوع کارت‌خوان‌ها وقتی که کارت به نزدیکشان برسد با هر نوع فرکانس رادیویی کار می‌کنند. بسیاری از کارت‌خوان‌های غیرتماسی مخصوص پرداخت، کنترل دسترسی فیزیکی و برنامه‌های کاربردی حمل‌ونقل طراحی شده‌اند. پروتکل غالب تحت ISO۱٤٤۳ با MIFARE است که از استاندارد EMV پیروی می‌کند.

(شکل شماره ۷ – کارتخوان غیرتماسی)

ارتباط

یک کارت‌خوان تماسی روش ارتباطی با PC تعریف شده است. این روش‌ها شامل پورت سریال RS ۲۳۲، پورت USB، سوراخ PCMCIA، سوراخ فلاپی دیسک، پورت‌های موازی، رابط IRDA و کیبورد و رابط بلوتوث کیبورد بیسیم است. برخی از کارت‌خوان‌ها مانند کارت‌خوان سه‌وجهی تعبیه‌ای مگ‌تک، بیش از یک نوع کارت را حمایت می‌کنند. این کارت‌خوان‌ها عملیات خواندن نوار تماسی و غیر تماسی مغناطیسی را در یک دستگاه پشتیبانی می‌کنند.

کارت‌خوان و ترمینال در ارتباطات کارت

همه کارت‌ها و کارت‌خوان‌ها از استاندارد ISO ۷۸۱۶-۳ که یک مجموعه استاندارد از دستورات توان‌ساز-ارتباطی کارت‌های CPU تابعیت می‌کنند.

این دستورات، به نام APDUs (پروتکل کاربردی واحد داده‌ها) را می‌توان در سطح بسیار پایین اجرا کرد یا آن را می توان بصورت فایل آغازگر در APIs قرارداد که بدینوسیله کاربر می‌تواند از یک برنامه، فرمان‌ها را به کارت‌خوان بفرستد.

کارت‌خوان با کارت ارتباط برقرار می‌کند در حالیکه به درخواست وارد شده پاسخ می‌دهد.

از دیدگاه فنی، کلید انتخابی APIs هستند این لایه‌های نرم‌افزاری، برای ایجاد ارتباط با کارت‌های هوشمند و کارت‌خوان‌های بیش از یک تولیدکننده برنامه کاربردی موثر فراهم می‌کنند. آنها به طور معمول در شکل های C ، C ++ یا C # هستند و هدر فایل در آن گنجانده شده است. بسیاری از کارت‌خوان‌های کارت هوشمند برای حافظه کارت‌ها، درایو خاص یا APIs دارند. برای کارت‌های پردازنده استاندارد ISO ۷۸۱۶ رابط PC / SC اغلب به کار می‌رود، اما محدودیت‌هایی دارد. این مسئله حائز اهمیت است بویژه اگر هر دو کارت‌حافظه و ریزپردازنده موجود باشد که در همان سیستم استفاده شوند. برخی از APIs به طراح نرم‌افزار توانایی انتخاب کارت‌خوان از بین چند فروشنده متعدد را می‌دهد.

موارد زیر از فرمان‌های تابع برای انتقال APDUs و توابع آنها هستند:

- انتخاب کارت‌خوان
- اتصال کارت‌خوان
- قطع کننده کارت‌خوان
- اتصال کارت
- فرمان‌های مقدم برای کارتخوانها و کارتهای خاص
- اجازه فرمان‌های ISO با استفاده از فرمت‌های استاندارد ISO که مورد تصویب کارت‌ها باشد.

- اجازه فرمان‌های ISO برای ارسال به کارت با استفاده از ساده‌سازی و میانبر فرمت مانند (CardLogix Winplex® API)

توسعه نرم‌افزارهای کاربردی

توسعه برنامه‌های کاربردی کامپیوتر برای کارت‌خوان‌ها با استاندارد کامپیوتر شخصی یا کارت هوشمند (PC/SC) ساده شده‌اند. این استاندارد توسط همه سیستم عامل‌های اصلی پشتیبانی می‌شود. مشکل با روش (PC/SC) این است که تمام توابع کارت‌خوان‌ها را پشتیبانی نمی‌کند که توسط تولیدکنندگانی چون کنترل LED و قفل کارت ارائه شده‌اند. هنگامی که از درایوها فقط برای هرکارت‌خوان سازنده استفاده می‌شود هیچ ارتباطی در توابع کارت وجود ندارد.

انتخاب بهتر، ارتباط برنامه کاربردی برنامه نویسی (APIs) است که بخشی از کیت طراحی نرم‌افزار (SDKs) است که خانواده کارت‌های سازنده را پشتیبانی می‌کند. این کیت‌ها را برای انواع مختلف کارت‌های سازنده بررسی کرد که توسط M.O.S.T پشتیبانی می‌شود و ابزارهای هوشمند از کارت لوجیکس مثال خوبی برای کارت‌های هوشمند شکیل SDK است.

ترمینال ها

برخلاف کارت‌خوان‌ها، ترمینال‌ها خیلی شبیه به کامپیوترPC با ویژگی سیستم‌عامل و ابزار توسعه هستند. ترمینال‌ها اغلب برای استفاده در مواردی چون امنیت، انفورماتیک سلامت POS (نقطه فروش) مشخص هستند. اتصال در ترمینال به طور معمول از طریق پروتکل کنترل انتقال یا پروتکل اینترنت (TCP-IP) و یا شبکه GSM انجام می شود. بسیاری از ترمینال‌های امروزی ویژگی OS های را عادی دارند که قابلیت استقرار آسان‌تر نوارهای داده با ویندوز CE یا انتشار با Linux دارند.

استاندارد کارت هوشمند

در ابتدا، ویژگی‌های ارتباطی و شناسه استفاده از تراشه استانداردهای کارت‌هوشمند جاسازی شده و داده ها از طریق خواص فیزیکی، کنترل می‌شوند. تقریباً همه استانداردها به ۳، ۲، ۱-۷۸۱۶ ISO بعنوان یک مرجع مبنا ارتباط دارد.

سازمان بین المللی استاندارد (ISO)

(ISO) از طریق یک مرحله آزاد، برای همه بخش‌ها، استانداردهای داوطلبانه ایجاد می‌کند.

۷۸۱۶ ISO یک استاندارد بین المللی برای کارت‌های یکپارچه مدار هستند (عموماً بعنوان کارت هوشمند شناخته شده‌اند) که با استفاده از اتصالات الکتریکی روی کارت و همچنین کارتی که با کارت‌خوان و ترمینال‌ها بدون اتصال ارتباط برقرار می‌کند، مانند تکنولوژی فرکانس‌های رادیویی (RF یا غیر تماسی).

کسانی که علاقه‌مند به درک فنی کارت‌های هوشمند هستند نیازمند آشنایی با چیزهایی هستند که ISO۷۸۱۶، ISO۱٤٤۳ پوشش نمی‌دهند و همچنین آنچه را که پوشش می‌دهند. نسخه‌هایی از این استانداردها را می‌توان از طریق موسسه ملی استاندارد آمریکا (ANSI) خریداری کنند. نسخه‌هایی از استاندارد بین‌المللی بر روی وب سایت ISO برای فروش قراردارند.

ویژگی‌های خاص برنامه با بسیاری از سازمان های بزرگ و گروه‌ها که پیشنهاد استانداردهای خود را ارائه کرده‌اند مورد بحث است.

گسترش سیستم قابلیت همکاری کارت باید در سطوح مختلفی اعمال شود:

۱- خود کارت

۲- پایانه‌های دسترسی کارت (کارت‌خوان‌ها)

۳- شبکه

٤- سیستم‌های خود صادرکنندگان کارت

قابلیت همکاری کارت سیستم آزاد را از طریق انطباق با استانداردهای بین‌المللی می‌توان بدست آورد.

حامیان مالی سایت متعهد به انطباق با استانداردهای ایمنی ISO وITSEC و همچنین طرح‌های صنعتی EMV و MULTOS ، چارچوب کارت آزاد و ویژگی های PC/SC هستند.

حامیان مالی این سایت به انطباق با استانداردهای امنیتی ISO و ITSEC و همچنین طرح‌های صنعت مانند EMV، پلت فرم جهانی و مشخصات کامپیوترPC/SC متعهد هستند.

این سازمان‌ها در استاندارد کارت هوشمند فعال هستند. استانداردهای زیر و سازمان‌هایی که حفظ آنها در صنعت کارت‌های هوشمند رایج ترین هستند:

ISO/IEC یکی از اعضاء تنظیم کننده تکنولوژی استاندارد در سراسر جهان، از جمله کارت‌های پلاستیکی است. استانداردهای اولیه برای کارت‌های هوشمند ISO IEC ٧٨١٦، ISO IEC ١٤٤٤٣، ISO IEC ١٥٦٩٣ و ISO IEC ٧٥٠١ هستند.

استاندارد ISO/IEC ٧٨١٦

ISO/IEC ٧٨١٦ استاندارد بین المللی چند بخشی است که به چهارده بخش قسمت شده‌است. قطعات ١ ، ٢ و٣ ISO/IEC ٧٨١٦ تنها با کارت هوشمند تماسی سر و کار دارد و جنبه‌های مختلف کارت‌ها و ارتباط‌های آنها، از جمله ابعاد فیزیکی کارت، رابط برق و پروتکل‌های ارتباطی را تعیین می‌کند. استاندارد ISO/IEC ٧٨١٦ قطعات ٤، ٥، ٦، ٨، ٩، ١١، ١٣ و ١٥ به انواع کارت های هوشمند (هم تماسی و غیر تماسی) مربوط می‌باشد. آنها ساختار منطقی کارت را معین می‌کنند (فایل‌ها و عناصر داده ها)، دستورات مختلفی توسط رابط برنامه‌نویسی برای استفاده عمومی، مدیریت برنامه، تایید بیومتریک، خدمات رمزنگاری و نامگذاری برنامه استفاده شده‌است. قسمت ١٠ استاندارد ISO/IEC ٧٨١٦ توسط کارت‌های حافظه برای برنامه‌های کاربردی مانند کارت‌های تلفن پیش پرداخت و یا دستگاه‌های فروش‌خودکار استفاده می شود.

قسمت ۷ استاندارد ISO/IEC ۷۸۱٦ سیستم پایگاه داده امن برای کارت‌های هوشمند مبتنی بر رابط SQL تعریف می کند (SCQL).

استاندارد ISO/IEC ١٤٤٤٣

ISO/IEC ١٤٤٤٣ یک استاندارد بین المللی است که ارتباط مجاورت نزدیک کارت غیرتماسی هوشمند را تعریف می‌کند. از جمله ارتباط فرکانس رادیویی (RF)، ارتباط برق و پروتکل‌های ارتباطات و ضد تصادم. کارت شکایت استاندارد ISO/IEC ١٤٤٤٣ در MHz ١٣/٥٦ اجرا می شود و یک دامنه فرآیند ۱۰ سانتیمتری (۳/۹٤ اینچ) دارد. استاندارد ISO/IEC ١٤٤٤٣ عمدتاً کارت هوشمند غیر تماسی است که برای ترانزیت مالی، برنامه‌های کاربردی دسترسی کنترل استفاده می‌شود. در ضمن برای عبور الکتریکی و در کارت FIPS PIV ۲۰۱ استفاده می شود.

استاندارد ISO/IEC ١٥٦٩٣

استانداردها را برای مجاورت کارت‌ها تعریف می‌شوند. به خصوص استاندارد ISO/IEC ١٥٦٩٣ برای ویژگی‌های فیزیکی، نیروی فرکانس رادیویی، پیغام ارتباطی، ضدبرخورد، و پروتکل انتقالی برای مجاورت کارت تا حداکثر ۱ متر(تقریباً ۳/۳ فوت) ایجاد می‌کند.

این نوع استاندارد، برای اسناد سفری که قابل خواندن در دستگاه کارت خوان باشند استانداردی تعریف می‌کند و در مکان‌شناسی کارت‌هوشمند توصیه‌های روشن مطرح می‌کند.

سازمان بین‌المللی هوایی کشور (ایکائو)

ایکائو در مورد مسائل استانداردسازی و خصوصیات دستگاه کارت‌خوان اسناد سفری مانند گذرنامه، ویزا و اسناد سفری رهنمودهایی دارد. ایکائو مشخصات گذرنامه الکتریکی را با استفاده از یک تراشه هوشمند غیرتماسی بطور ایمن در داده‌های مسافر منتشر می کند.

استانداردهای پردازش اطلاعات فدرال (FIPS)

استاندارد (FIPS) توسط بخش امنیت کامپیوتر در موسسه ملی استاندارد و فناوری توسعه یافت. استانداردهای فیپس برای محافظت از دارایی‌های فدرال، از جمله کامپیوتر و سیستم‌های ارتباطات از راه دور طراحی شده‌اند. استانداردهای فیپس در تکنولوژی کارت‌های هوشمند بکار می‌روند و برای استانداردهای امضاء دیجیتالی، استانداردهای رمزدارکردن و امنیت لازم برای مدل‌های رمزی، مناسب هستند.

FIPS ۱٤۰(۱-۳)

نیازمندیهای امنیتی که در (۳-۱) FIPS ۱٤۰ وجود دارند مربوط به مواردی چون طراحی ایمن و اجرای ماژول رمز نگاری است، به خصوص در مشخصات ماژول رمزنگاری، درگاه ماژول رمزنگاری و ارتباطات، نقش، خدمات، و احراز هویت، مدل محدود دولتی، امنیت فیزیکی، محیط قابل استفاده، مدیریت کلید رمزنگاری، ارتباط الکترومغناطیسی، سازگاری الکترومغناطیسی، (EMI / EMC)، خودآزمونی‌ها، ضمانت طراحی و کاهش حملات دیگر.

FIPS ۲۰۱

این خصوصیت تمام جنبه‌های کارت‌های چند منظوره را در سیستم مدیریت هویت در سراسر دولت ایالات متحده آمریکا پوشش می‌دهد.

یوروپی، مستر کارت، ویزا

یوروپی، مستر کارت و ویزا، شرکت ای ام وی، وی ال ال سی را تشکیل دادند و مشخصات کارت مدار مجتمع در سیستم‌های پرداخت را درست کردند. این مشخصات به ISO ۷۸۱٦ مربوط است و یک اساس فنی مشترک برای کارت و سیستم پیاده‌سازی اعتبار ایجاد می‌کند. کارت مدار مجتمع برای سیستم‌های پرداخت را می‌توان از طریق یک بانک عضو ویزا، مستر کارت و یوروپی فراهم کرد.

استاندارد PC/SC

یک استاندارد در سطح جهانی برای کارت‌ها و کارت‌خوان‌ها با نام PC/SC وجود دارد. این استاندارد تنها درکارت‌های تماسی CPU صدق می‌کند. همچنین نسخه ۲ ارتباط کارت را به پین اداره می‌کند. اپل، اوراکل، سان، لینوکس و مایکروسافت این استاندارد را پشتیبانی میکنند.

مایکروسافت در خدمات کارت‌هوشمند خود از استاندارد PC/SC استفاده می‌کند که بعنوان چارچوبی است که بسیاری از مکانیزم‌های امنیتی را پشتیبانی می‌کند. در حال حاضر استاندارد PC/SC یک رابط میان افزار نسبتاً رایج برای برنامه‌های کاربردی لوگون PC است. این استاندارد مجموعه بسیار کوچک از اجزاء میان-افزارها است که به بیشتر کارت‌خوان‌ها اجازه فعل و انفعالات کارت‌خوانی می‌دهد.

کمیته استاندارد اروپا (CEN) و موسسه استانداردهای مخابراتی اروپا (ETS)

(CEN) و (ETSI) بر ارتباطات راه دور تمرکز دارند. مانند GSM SIM برای تلفن های همراه GSM ۱۱/۱۱ و ET ۱۳۰۰۰٤٥.

بیمه سلامت حمل و نقل و ترابری و قانون پاسخگویی (HIPAA)

(HIPAA) با استانداردهای بین‌المللی برای پیاده سازی یک سیستم ایمن الکتریکی تراکنش در ایالات متحده وفق دارد. نمونه تراکنش‌ها تحت تاثیر این درخواست‌ها است: ثبت نام، واجد شرایط بودن، پرداخت و هماهنگی منافع. کارت‌های هوشمند توسط الزامات HIPAA متعلق به کارت و حریم خصوصی بیمار اداره می‌شود.

استاندارد ارتباطات IC

استانداردهای ارتباطات IC قبل از اینکه از تراشه برای کارت‌هوشمند استفاده شود، برای حافظه‌های غیرفرار وجود داشت. این ویژگی مخصوصاً در ارتباطات ۱۲C و SPI EEPROM اجرا می‌شود.

سیستم جهانی ارتباطات تلفن همراه (GSM)

استاندارد GSM در صنعت تلفن‌همراه کاربرد دارد و از کارت‌های‌هوشمند در آن استفاده می‌شود که ماژول شناسایی مشترک نامیده می شوند (SIM) که با اطلاعات ضروری اعتباری GSM یک تلفن همراه پیکربندی می‌شوند. در نتیجه اجازه می‌دهد در هر زمان که تلفن داخل پوشش یک شبکه مناسب قرار گرفت خدمات دریافت کند. این استاندارد، توسط موسسه استاندارد مخابرات از راه دور اروپا اداره می‌شود. دو استاندارد رایج این نوع کارت‌ها ۱۱/۱۱ و۱٤ /۱۱ است.

پلت فرم جهانی (GP)

پلت فرم جهانی (GP) ارتباط بین‌المللی، غیرانتفاعی است. هدف آن ایجاد، حفظ و وفق استانداردهای گرداننده برای همکاری زیرساخت‌های کارت‌های هوشمند، دستگاه‌ها و سیستم‌ها است که توسعه را شتاب داده، آسان کرده، و مدیریت نرم افزار کاربردی درهمه صنایع را بکار گیرد. استاندارد GP تقریباً توسط همه

بانک‌های دنیا برای بارگذاری داده‌های رمزی، کارت جاوا پذیرفته شده است. استاندارد مکانیزم و سیاست-هایی را برقرار می‌کند که ایمنی کانال‌های ارتباطی را با اعتبار برقرار می‌کند.

پرداخت را می‌توان از طریق یک بانک عضو ویزا، مسترکارت و یوروپی فراهم کرد.

معیارهای مشترک (CC)

معیارهای مشترک یک چارچوب ارزیابی امنیتی بین المللی است که ارزیابی روشن و قابل اعتماد از قابلیت-های امنیتی محصولات فناوری اطلاعات IT شامل IC، سیستم عامل کارت هوشمند و نرم‌افزار کاربردی فراهم می‌کند. این معیار مشترک ارزیابی مستقل از توانایی یک محصول مهیا می‌کند تا متناسب با استانداردهای امنیتی باشد. مشتریان آگاه به امنیت، مانند دولت‌های ملی بطور فزاینده صدور تصدیقCC را برای انجام خرید ضروری میدانند می‌توانند. از آنجایی که شروط تصدیق بوضوح مشخص شده‌اند؛ فروشندگان، برای ارائه محصول نیازهای امنیتی بسیار خاص نیز اعمال کنند.

استانداردهای بیومتریک

بسیاری از سیستم های جدید راه اندازی ID از هر دو نوع کارت‌های بیومتریک و هوشمند برای بهبود امنیت و حفظ حریم خصوصی سیستم ID استفاده می‌کنند.

ANSI- INCITS ۳۵۸–۲۰۰۲

ANSI- INCITS ۳۵۸–۲۰۰۲ (استاندارد ۱– ۱۹۷۸٤ ISO/IEC)، BIO API رابط برنامه‌نویسی کاربرد بیومتریک یک بخش کلیدی از استانداردهای بین المللی است که سیستمهایی که ثبت نام و شناسه بیومتریک انجام می‌دهند را حمایت می‌کند تا دستگاه بیومتریک خدمات فن آوری و جمعیت شناسایی برای عملکرد مطلوب را اداره کند. در ضمن شکل‌های اولیه هندسی را نیز فراهم می‌کند که به برنامه کاربردی اجازه می‌دهد که بطور جداگانه در یک ایستگاه کاری کاربر، نمونه‌ها را در سرور تسخیر، ثبت نام، تائید و شناسایی

کند. چارچوب BIO API به Win۳۲، لینوکس، بیوتکس و وینس انتقال داده شده‌اند. باید دقت شود که برای یک محیط میکروکنترلر مطلوب نیست همانند آنهایی باشند که احتمالاً به کارت‌خوان کنترل درب دسترسی دارند یا داخل پردازنده یک کارت هوشمند قرار دارند. وقتی که کامپیوتر در دسترس استBIO API مناسب‌تر است.

ANSI- INCITS ۳۹۸

ANSI- INCITS ۳۹۸ چارچوب فرمت تبادل بیومتریک مشترک (CBEFF)

استاندارد ISO/IEC ۱۹۷۸۵ مجموعه‌ای از عناصر داده‌ها را که برای حمایت از فن آوری بیومتریک و تبادل اطلاعات ضروری هستند را تعریف می‌کند. این داده‌ها را می توان در یک فایل جداگانه قرار داد که اطلاعات بیومتریک را بین اجزاء مختلف سیستم‌ها یا بین خود سیستم‌ها تبادل کند. نتیجه قابلیت همکاری برنامه‌های کاربردی بیومتریکی را توسعه می‌دهد و سیستم ها توسط فروشندگان مختلف با اجازه تبادل داده‌های بیومتریک توسعه می‌یابد. این خصوصیت یک نسخه اصلاح شده (و اثبات شده) از CBEFF اصلی است. فرمت فایل تبادل بیومتریک عادی، در اصل با عنوان NISTIR ٦٥٢٩ منتشر شد.

ANSI-INCITS استانداردهای تبادل فرمت داده های بیومتریک

این استاندارد یک رشته استانداردهایی را ایجاد کرده که تبادل فرمت داده‌های بیومتریک را مشخص می‌کند. این استانداردها داده‌هایی را برای ثبت تبادل فرمت است جهت ذخیره سازی، ثبت و انتقال اطلاعات از یک نمونه در ساختار داده های CBEFF تعیین می‌کنند. ANSI-INCITS ا ستانداردهای تبادل داده‌ها را منتشر کرده در زیر آورده شده است. فهرست معادل‌هایی برای ایزو در هر استاندارد در زیر مشاهده می‌شود:

- ANSI-INCITS ۳۷۷–۲۰۰٤ – الگوی انگشت بر اساس فرمت تبادل
- ANSI-INCITS ۳۷۸–۲۰۰٤ – فرمت دقیق انگشت برای تبادل داده‌ها
- ANSI-INCITS ۳۷۹–۲۰۰٤ – فرمت تبادل تصویر عنبیه
- ANSI-INCITS ۳۸۱–۲۰۰٤ – فرمت تبادل بر اساس تصویرانگشت
- ANSI-INCITS ۳۸۵–۲۰۰٤ – فرمت شناخت صورت برای تبادل داده‌ها
- ANSI-INCITS ۳۹۵–۲۰۰۵ – فرمت تبادل بر اساس تصویر امضاء
- ANSI-INCITS ۳۹٦–۲۰۰٤ – فرمت تبادل قالب هندسی دست

ISO/IEC ۱۹۷۹٤

ISO/IEC ۱۹۷۹٤ سری فرمت تبادل داده‌های بیومتریک است.که دارای ۹ قسمت است: قسمت اول چارچوب است، قسمت دوم داده‌های دقیق انگشت، قسمت سوم طرح طیفی انگشت، قسمت چهارم داده تصویر انگشت، قسمت پنجم داده های تصویر چهره، قسمت ششم تصویرعنبیه، قسمت هفتم امضاء، قسمت هشتم الگوی اسکلت انگشت و قسمت نهم اطلاعات تصویر عروقی را تعریف می‌کند.

توسعه و برنامه ریزی کارت هوشمند

طراحی سیستم کارت هوشمند برای موفقیت و برای جلوگیری از مشکلات، نیاز به برنامه‌ریزی از پیش دارد. بنابراین بر روی سیستم جدید باید دیاگرام جریان بروشنی وارد شود. اولین پرسش این خواهد بود که آیا کارت و سیستم اطلاعات یا اعتبار یا هر دو را تبادل می‌کنند. اگر کلیدها یا اعتبار را ذخیره کند (مثلاً کارت هدیه یا بلیط‌های ورزشی) غیر از داده‌های محض سیستم جزییات بیشتری در طراحی نیاز است. وقتی اطلاعات روی یک کارت ترکیب می‌شود، مسائل دیگری بوجود می‌آید. کلید موفقیت اشغال‌کردن

سیستم با ویژگی‌هایی که کاربر را گیج می‌کند و در مدیریت مشکلات بوجود می‌آورد. برای پیاده سازی درست یک سیستم هوشمند باید کاربران به سوالات زیر بتوانند پاسخ دهند.

- آیا یک مورد تجاری روشن از جمله عوامل مالی و رفتاری وجود دارد؟
- آیا سیستم تک یا چند منظوره خواهد بود؟
- چه نوع اطلاعاتی را می خواهید درون کارت ذخیره کنید؟
- برای هر برنامه چقدر حافظه لازم است؟
- اگر چند منظوره است چگونه داده‌ها از هم جدا خواهند شد؟
- آیا اطلاعات داده از یک پایگاه به دست آمده است؟ یا در زمانهای مختلف بارگیری شده است؟
- آیا این اطلاعات به صورت همزمان در یک پایگاه داده اقامت خواهد کرد؟
- چند کارت مورد نیاز است؟
- آیا کارت یا سازمان فروشندگان شناسایی خواهند شد؟ زمان های تقدم چیست؟

برنامه‌ریزی امنیتی

- نیازمندی‌های امنیتی چیست؟
- آیا همه برنامه‌ها یا فقط تعدادی نیازمند ایمن سازی هستند؟
- چه کسانی به اطلاعات دسترسی خواهند داشت؟
- چه کسی مجاز به تغییر این اطلاعات است؟
- با چه روشی می‌توان این داده‌ها را ایمن کرد؟ مثلاً رمزگذاری، کلمه عبور میزبان، رمز عبور کارت، پین ها یا همه این ها ؟
- آیا کلیدها یا پین‌ها باید توسط مشتری فعال شود یا سیستم ؟
- چه فرمی از نسخه کنترل لازم است ؟

نرم‌افزارهای اعتباری

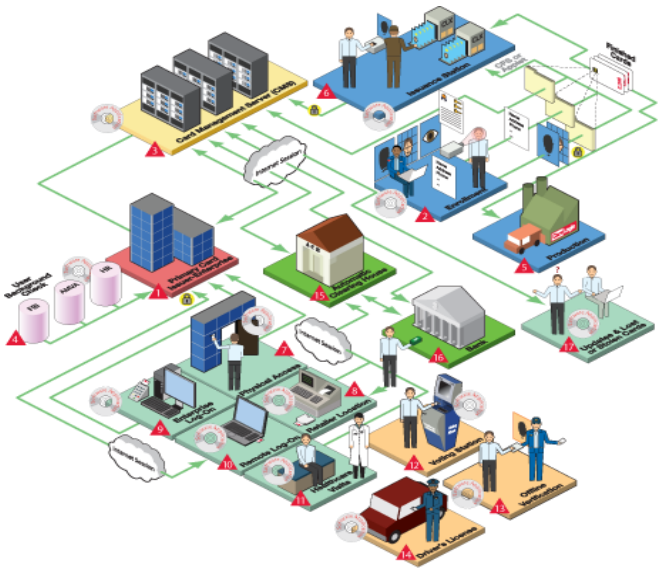
- آیا اعتبار کارتها باید مجدد بار گذاری شود و یا مجدداً استفاده شود؟
- چگونه کارت توزیع شود؟
- چگونه کارت ها فعال شوند و بار گذاری شوند ؟
- چه نوع کارت قابلیت ردیابی باید پیاده سازی شود؟
- ارزش حداقلی و حداکثری ذخیره روی کارت ها چقدر است ؟
- آیا یک سیاست بازپرداخت وجود دارد؟

صدور همگانی

- چند نوع چاپ در صدور کارت‌ها وجود دارد؟
- چه کسی کار چاپ را انجام می‌دهد؟
- چه چیزی برای کارت نیاز است مثلاً : امضاء، نوار مغناطیسی، برجسته سازی.

سیستم‌های کارت چندمنظوره

نمودار سیستم های کارت چندکاربرد بصورت زیر ترسیم می شود:



(شکل شماره ۸ – سیستم های چند منظوره)

سیستم‌های توزیع بزرگ احتیاج به برنامه‌ریزی از پیش دارد تا قابل اجرا شوند. کارت‌های هوشمند اغلب بعنوان چسب در بین برنامه‌های نرم‌افزارهای عمل می‌کنند و از پوسته استفاده می‌کنند. در زیر یک مثال از کارت چند منظوره آورده شده است که توسط شرکت های بزرگ و یا دولت صادر شده‌اند. همه جا می‌بینید که یک سی دی برنامه نرم‌افزار جدا و متفاوت است که متقابلاً در داده‌ها و خدمات کارت اثر می‌کند.

اولین گام مهم در این نوع، برنامه‌ریزی برای درک الزامات داده‌ها روی کارت است چون با برنامه نرم‌افزار غیر متجانس که برنامه با آن اجرا می شود مربوط می‌باشد.

ساخت یک سیستم هوشمند که اعتبار را ذخیره می‌کند مثلاً کارت هدیه یا بلیط‌های ورزشی، باز خرید یا معادل پول نقد نیاز به توجه به جزییاتی دارد که در سیستم های مدیریت اطلاعات ضروری نیست. مهمترین

جزییات کارت اعتباری هوشمند این است که کارت و برنامه که توسط کاربر دریافت می‌شود قانع‌کننده باشد و سویچ را به دیگر گزینه‌های پرداخت برتر می‌داند.

فصل چهارم

امنیت در کارت‌های هوشمند

امنیت کارت هوشمند، قسمت ۱

کارت‌های هوشمند، با استفاده از سیستم‌های محاسباتی و تجارتی، فایده فراوانی از لحاظ قابل حمل و ایمن‌بودن داده‌ها و اعتبار فراهم می‌کنند. وقتی کارت‌های هوشمند با سیستم ادغام می شوند، نوع مدیریت ایمنی خود را به سیستم معرفی می‌کنند، به طوریکه افراد از طریق برنامه‌های مختلف بطور وسیع به داده‌های کارت دسترسی پیدا می کنند.

امنیت اطلاعات چیست؟

امنیت اطلاعات، برنامه محاسباتی است برای اطمینان از ایمنی و حفظ حریم خصوصی داده ها، که از طریق مدیریت ذخیره‌سازی و توزیع آن مورد استفاده قرار می‌گیرد. امنیت اطلاعات هر دو مفاهیم فنی و اجتماعی را دارد. مفاهیم فنی کار، رسیدگی به این پرسش را بعهده دارند که امنیت اطلاعات "چگونه " و "چقدر" با یک هزینه معقول محاسبه می شود. مفـاهیم اجتماعی با موضوعاتی همچون آزادی فردی از قبیل: نگرانی‌های عمومی، استانداردهای قانونی و اینکه چگونه نیاز به حریم خصوصی باعث از هم گسیختگی آنها می‌شود. این بحث طیف وسیعی از گزینه‌ها را پیش روی مدیران تجاری، برنامه ریزان سیستم و برنامه‌نویسان قرار می دهد که به استراتژی امنیت کمک خواهد کرد. انتخاب نهایی به عهده طراح سیستم و صادرکننده می‌باشد.

عناصر امنیت اطلاعات

در اجرای یک سیستم امنیتی، تمام شبکه‌های داده‌ها با عناصر اصلی زیر سرو کار دارند:

- **سخت افزار**، از جمله سرورها، دستگاه‌های ذخیره سازی انبوه تکراری، کانال‌ها و خطوط ارتباطی، رمزهای سخت افزاری (کارت های هوشمند) و دستگاه‌های مکان یاب از راه دور (بعنوان مثال: مشتریان کم جمعیت و یا لوازم اینترنتی) بعنوان رابط کاربر و کامپیوتر عمل می‌کنند.
- **نرم افزار**، از جمله سیستم عامل، سیستم‌های مدیریت پایگاه داده‌ها، ارتباطات و برنامه کاربردی-امنیتی.
- **داده ها**، از جمله پایگاه‌های داده‌های مشتریان، اطلاعات مربوط به مشتریان.
- **پرسنل معمولی**، به عنوان تهیه کننده یا کاربر داده‌ها،
- **پرسنل حرفه‌ای**، کارمند دفتری، پرسنل اداری و کارمندان کامپیوتر.

مکانیزم امنیت داده‌ها

کار با عناصر فوق ، یک سیستم موثر امنیت داده‌ها با مکانیزم‌های کلیدی زیر را به وجود می‌آورد تا به موارد زیر پاسخ دهد:

- **آیا داده ها وارد شده سالم هستند؟** (درستی داده‌ها) مکانیزم، اطمینان حاصل می‌کند که آیا داده‌ها مفقود یا خراب نشده باشند.
- **آیا داده‌های گمشده یا خراب از شخص درستی بدست آمده اند؟** (تعیین هویت) هویت کاربر و سیستم را مشخص می‌کند.
- **آیا می‌توان دریافت دادها وهویت فرستنده را تایید کرد؟** (عدم انکار)
- **آیا می‌توان داده‌ها را خصوصی کرد؟** (راز داری) دسترسی فرستنده و گیرنده به داده‌ها را تضمین می‌کند. اینکار با ایجاد تکنیک‌های رمزی متفاوت برای امنیت داده‌ها انجام می‌گیرد.

- **آیا می‌توان در صورت انتخاب، داده‌ها را به اشتراک گذاشت؟** (اختیار و وکالت) می‌توان امتیازهای دسترسی را مشخص و مدیریت کرد.
- **آیا می‌توان تاییدکرد که سیستم به درستی کار می‌کند؟** (بازرسی و ثبت وقایع) ایمنی سیستم و رفع عیوب و مانیتورینگ را تامین می‌کند.
- **آیا می‌توان سیستم را مدیریت کرد؟** (مدیریت) اجازه اداره امنیت سیستم را می‌دهد.

امنیت کارت هوشمند ، قسمت ۲

درستی داده‌ها

این تابع ویژگی‌های مدارک و تراکنش‌ها را تایید می‌کند. ویژگی‌های هر دو از نظر محتوا و صحت بررسی و تایید می‌شوند. درستی داده‌ها از طریق رمزنگاری الکترونیکی صورت میگیرد که یک هویت منحصر به فرد به داده‌ها اختصاص داده می‌شود مانند اثر انگشت. هرگونه تلاش برای تغییر این علائم هویتی، تغییر پرچم‌ها و مداخله محسوب می‌شود.

احراز هویت

هویت درست افراد را از نظر داده‌ها و اعتبار در یک تراکنش، بررسی و سپس تایید می‌شود. احراز هویت را در سیستم‌های احراز هویت، بوسیله شناسایی مکانیزم‌های استحکام و اینکه چند عامل برای تایید و شناسایی استفاده شده‌اند محاسبه می‌شوند. در یک سیستم PKI یک امضای دیجیتالی، داده‌ها را در منشاء خود با تولید یک هویت که توسط دو طرف تراکنش مورد تایید قرار گیرد، ایجاد میکند. رمزگذاری یک الگوریتم دارد که امضای دیجیتالی تولید می‌کند.

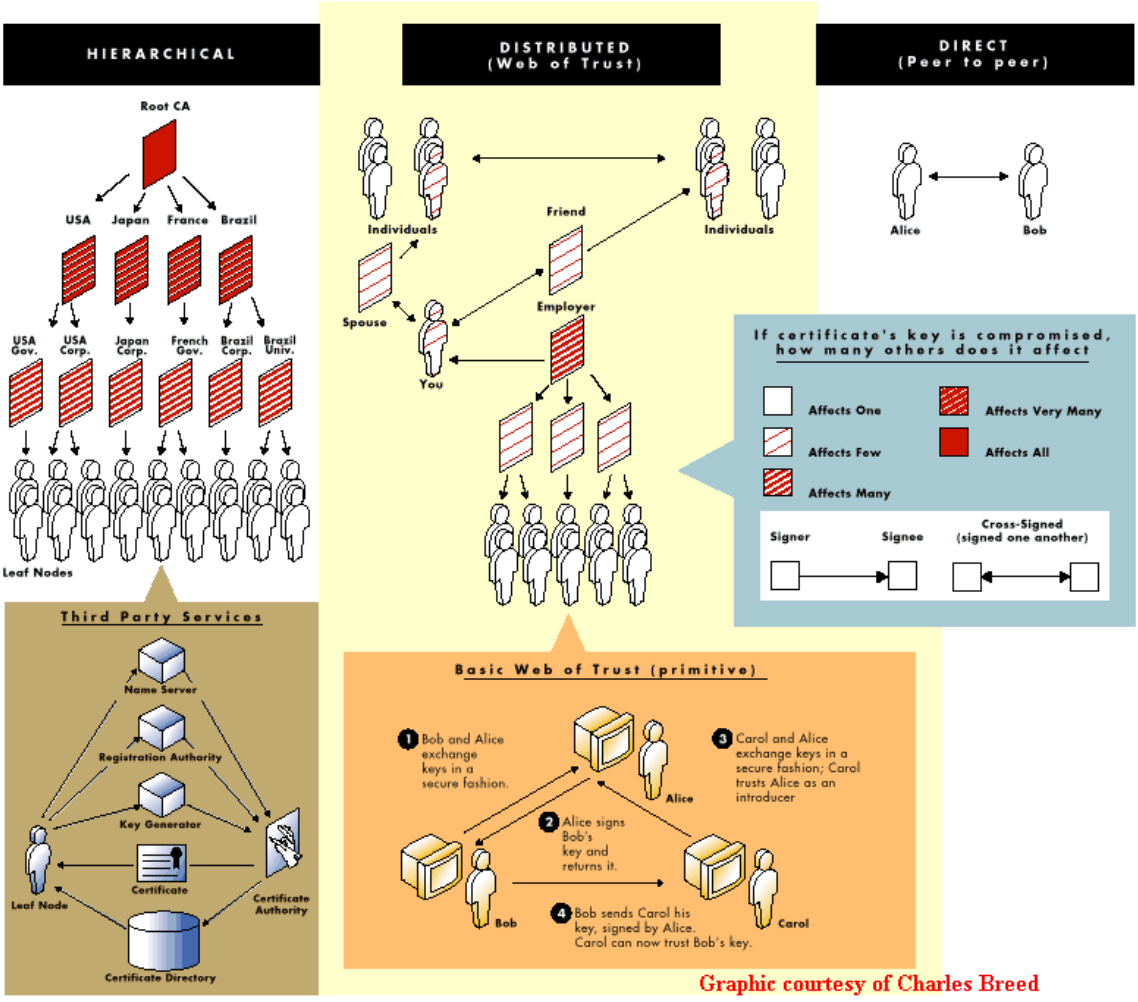
غیرمتجانس‌ها

تراکنشی را حذف می‌کند که امکان عدم پذیرش یا باطل شدن دارد، و این کار را با جا دادن یک امضای-دیجیتالی انجام می‌دهد که نفر سوم می‌تواند درستی آنرا تایید کند. مشابه این روش در پست الکترونیکی

ثبت شده است. که دریافت‌کننده داده‌های آنرا بصورت جدیدی مطرح، امضای دیجیتالی را تایید می‌کند و هر دو را با هم مقایسه کرده تا ببیند آیا آنها با هم هماهنگ هستند یا خیر؟

اجازه و نمایندگی

اجازه، مرحله‌ای است که دسترسی به داده‌های خاص را در یک سیستم نمایندگی به نفر سوم می‌دهد تا هر یک از کاربران را تایید و مدیریت کند.



(شکل شماره ۹ – تصویر اجازه مرحله‌ای)

حسابرسی و ورود

حسابرسی و ورود، یک بررسی مستقل و ثبت سوابق و فعالیت ها است که برای اطمینان از انطباق با کنترل، سیاست و روش‌های عملیاتی، برقرار شده و هر گونه تغییرات در کنترل‌ها، سیاست و یا روش‌ها، ایجاد شده‌است.

مدیریت

آیا نظارت و طراحی عناصر و مکانیزم‌های بالا و پایین نیاز به مدیریت دارد؟ مدیریت کارت نیز به مدیریت صدور کارت، جایگزینی، بازنشستگی و همچنین سیاست حاکم بر سیستم نیاز دارد.

رمزنگاری و قابلیت اعتماد

قابلیت مورد اعتماد بودن استفاده از رمز، برای حفظ اطلاعات است. متن ساده از طریق یک الگوریتم به متنی رمزدار تبدیل می‌شود سپس رمز با استفاده از همان روش به متن ساده تبدیل می‌شود.

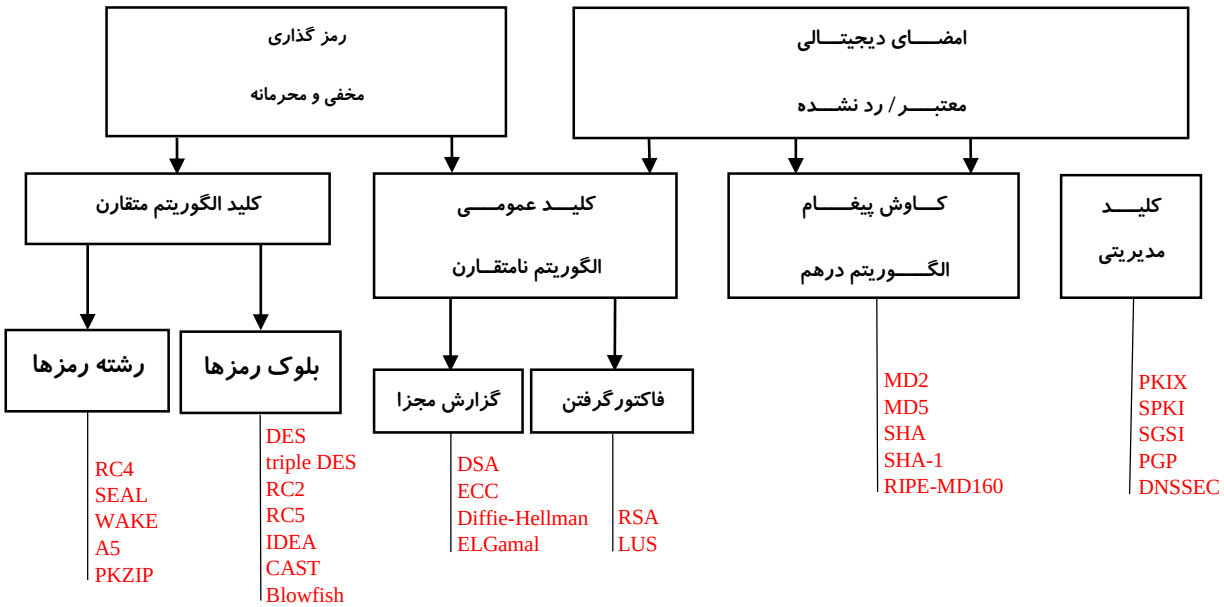
رمزنگاری یک شیوه باستانی حفاظت از اطلاعات است که سابقه آن به حدود ٤٠٠٠ سال پیش از میلاد باز می‌گردد. امروزه رمزنگاری در دنیای مدرن از اهمیت ویژه ای برخوردار است، به طوری که رمزنگاری به عنوان یک روش مؤثر برای حفاظت از اطلاعات حساس و شخصی به کار می‌رود. اطلاعاتی مانند اطلاعات طبقه بندی شده نظامی، اطلاعات حساس مؤسسات مالی، کلمات عبور که بر روی سیستم های کامپیوتری ذخیره شده اند و داده هایی که بر روی اینترنت و یا از طریق امواج رادیویی انتشار می‌یابند. رمزنگاری در کارت‌های هوشمند روشی است که داده‌ها را به یک فرم قابل خواندن توسط انسان به شکلی غیرخوانا تبدیل می‌کند، و سپس بازگشت به فرم قابل خواندن اصلی خود را انجام میدهد، تا دسترسی‌های غیر مجاز را دشوار سازد.

رمزنگاری در روش‌های زیر استفاده می‌شود:

- برای اطمینان از حریم خصوصی از طریق داده‌های مختلف رمزی
- برای اطمینان از درستی، از طریق شناسایی در مورد اینکه آیا داده‌ها با روش درست انجام شده‌است.
- برای اطمینان از بی‌همتایی داده‌ها، از طریق بررسی اصیل بودن و یا کپی نبودن از نسخه اصلی فرستنده است که با نسخه اصلی یک شناسه اصیل ضمیمه می‌شود.

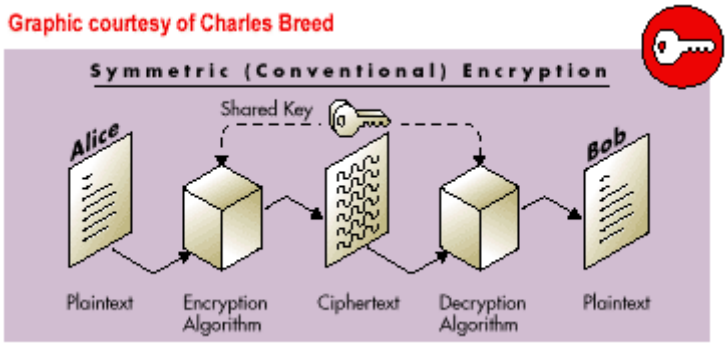
داده‌های اصلی ممکن است در یک فرم قابل فهم برای انسان باشد، مانند فایل متنی، یا ممکن است به صورت یک فرم قابل خواندن برای یک کامپیوتر باشد، مانند پایگاه داده‌ها، صفحات وب یا گرافیکی. داده‌های اصلی به نام داده‌های رمزی یا متن ساده معرفی میشوند. داده‌های اصلاح و تغییر داده شده را داده‌های رمزی یا متن رمزی می‌نامند. فرآیند تبدیل داده‌های غیر رمزی را رمزنگاری یا رمزگذاری و فرآیند داده‌های رمز گذاری به غیر رمزی را رمزگشایی می‌نامند.

مکانیزم امنیتی داده‌ها و الگوریتم مربوطه



(شکل شماره ۱۰ – نمودار مکانیزم امنیتی داده‌ها و الگوریتم مربوطه)

به منظور تبدیل داده‌ها، نیاز به یک الگوریتم رمزنگاری و یک کلید یکتا است. اگر همان کلید برای هر دو رمزگذاری و رمزگشایی استفاده شود کلید را، کلید مخفی می‌نامند و الگوریتم یک الگوریتم آن متقارن نامیده می‌شود. شناخته شده‌ترین الگوریتم متقارن DES می‌باشد. (استاندارد رمزگذاری داده‌ها)

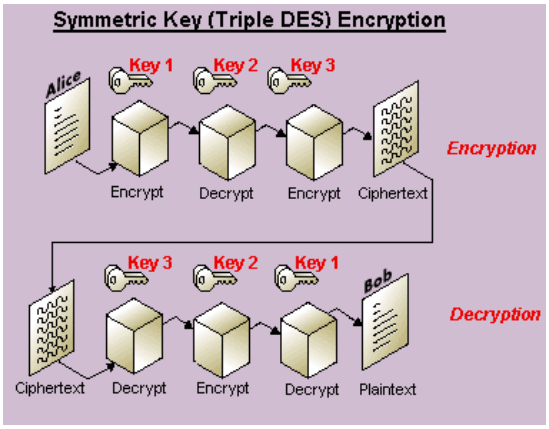


(شکل شماره ۱۱– الگوریتم متقارن)

استاندارد رمزگذاری داده‌ها (DES) در سال ۱۹۷۰ توسط شرکت IBM اختراع شد. در طول فرآیند استاندارد الگوریتم شدن، براساس توصیه‌های آژانس امنیتی ملی اصلاح شد. حدود بیست سال الگوریتم توسط رمزگذاران مطالعه شده است. درطول این مدت روش دیگری که الگوریتم را بشکند به جز تکنیک‌های بروت فورس منتشر نشده است. DES دارای کلید ٥٦ بیتی است که ۲٥٦ یا ۱۰۱٦ × ۷ تغییرات ممکن ارائه می‌دهد. تعداد بسیار کمی از کلیدهای ضعیف وجود دارند اما برای امتحان این کلیدها راه ساده‌ای وجود دارد و از آنها اجتناب می‌شود.

DES سه‌تایی روشی است که از DES استفاده می‌کند تا ایمنی بیشتری فراهم کند. DES سه‌تایی با دو یا نیز سه کلید می‌تواند انجام شود. از آنجایی که الگوریتم کار رمزگذاری و رمزگشایی را به ترتیب انجام

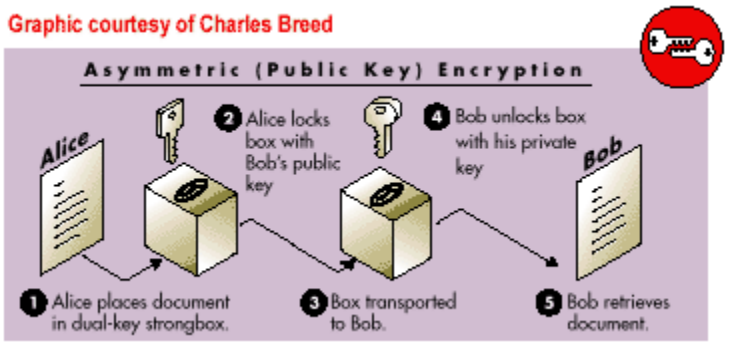
می‌دهد، گاهی اوقات آنرا EDE نیز می‌نامند. نمودار زیر DES سه تایی، در حالت سه کلیدی مورد استفاده رمزگذاری را نشان می‌دهد:



(شکل شماره ۱۲ – نمودار DES)

که به اینصورت عمل میکند که متن اصلی پس از سه بار رمزگذاری شدن از طرف آلیس ارسال می شود و سپس باب آن را پس از سه بار رمزگشایی می تواند بخواند.

اگر کلیدهای مختلف برای رمزگذاری و رمزگشایی استفاده شود الگوریتم را الگوریتم غیر متقارن می‌نامند. معروفترین الگوریتم غیر متقارن (RSA) است که از نام سه مخترع آن (ریوت، شامیر و ادل من) گرفته شده است. الگوریتم از دو کلید استفاده می‌کند که به آنها کلید خصوصی می‌گویند. این کلیدها از نظر ریاضی به هم وابسته هستند. در اینجا یک الگوریتم غیر متعارف نشان داده شده است:



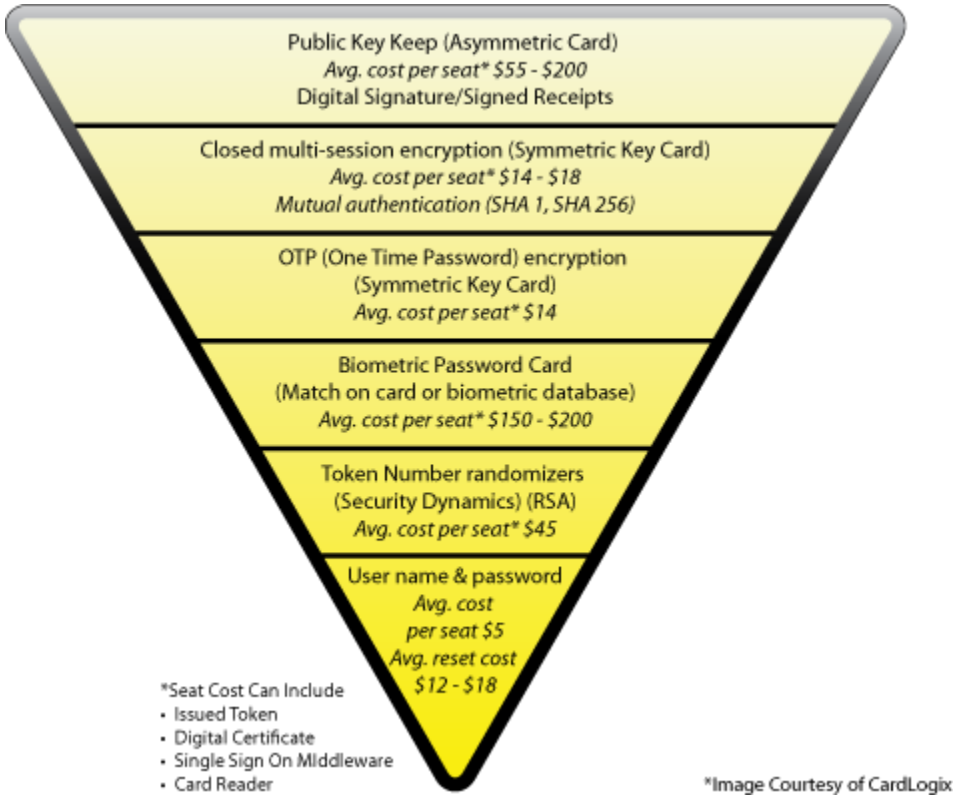
(شکل شماره ۱۳ – نمودار الگوریتمی غیر متعارف)

که به اینصورت عمل می‌کند که آلیس متن را در جعبه مجازی دو کلیدی قرار می‌دهد، سپس با کلید عمومی آن را قفل می‌کند. جعبه رمزگذاری شده را برای باب ارسال می‌کند و باب با استفاده از کلید خصوصی اش آن را باز می‌کند و متن رمزگشایی شده برایش خوانا می شود.

الگوریتم غیرمتعارف شامل محاسبات بسیار پیچیده‌ای است، بطور نمونه عاملیت اولیه ارقام. الگوریتم غیر-متعارف از یک کلید کوتاه الگوریتمی غیرمتعارف قویتر است. اما به دلیل پیچیدگی در علامت‌گذاری یک پیغام یا سند استفاده می‌شوند. بطور معمول از آنها در انتقال متن رمزگذاری استفاده نمی‌شود.

امنیت کارت هوشمند، قسمت ۳

صادرکننده کارت، باید تمام پارامترها را برای کارت و امنیت داده‌ها تعریف کند. دو نوع روش استفاده کارت‌ها برای امنیت سیستم داده‌ها وجود دارد، میزبان مبنا و کارت مبنا. سریعترین سیستم‌ها هر دو روش ها را بکار می برند.



(شکل شماره ۱٤ – نمودار هزینه)

امنیت سیستم میزبان مبنا

یک سیستم میزبان مبنا، کارت را بعنوان یک انتقال دهنده داده‌ها تلقی می‌کند. به همین علت کارت‌های حافظه مستقیم را می توان با بارآوری فراوان در بسیاری از سیستم‌ها بکار برد. همه داده‌ها از طریق کامپیوتر میزبان حفاظت می‌شوند. اطلاعات کارت ممکن است رمز گذاری شود اما هنگام انتقال به میزبان می تواند آسیب پذیر برای حمله باشد. یک روش معمول افزایش امنیت این است که یک کلید را بطور صریح (رمزگذاری نشده) با مرجع مخفی، به یک گروه کلیدهای درون میزبان معرفی شود که معمولاً شامل تاریخ و زمان است. هر وقت که کارت باز نویسی می‌شود، میزبان می‌تواند یک مرجع به کلیدها معرفی کند. باین ترتیب هر انتقال با دیگر انتقالات متفاوت است. اما قسمت‌هایی از کلیدها برای تجزیه و تحلیل هکرها واضح هستند. این امنیت را می‌توان با استفاده از کارت حافظه هوشمند افزایش داد که یک مکانیزم رمزعبور برای جلوگیری از خواندن داده‌ها، بصورت غیرمجاز است. متاسفانه کلمه عبور بروشنی می‌تواند ردیابی شود. آنگاه دسترسی به حافظه اصلی امکان پذیر می‌شود. این روش‌ها اغلب در شبکه می‌تواند داده‌ها را بطور منظم دسته‌بنـدی کرده، اعتبارات و استفاده کارت را مقـایسه کند و فهرست مشکلات کارت را جمع‌آوری کند.

امنیت سیستم کارت مبنا

این سیستم ها بطور معمول ریز پردازنده کارت مبنا هستند. یک کارت، یا سیستم رمز مبنا یک کارت را بعنوان یک دستگاه محاسباتی فعال تلقی می‌کند. تعامل بین میزبان و کارت می‌تواند مراحلی باشد که تعیین می‌کند آیا کارتی مجاز به این است که مورد استفاده در سیستم قرار گیرد. این فرآیند همچنین بررسی می‌کند که آیا کاربر قابل شناسایی، تایید است و آیا کارت اعتبار مناسب برای انجام یک تراکنش را دارد. کارت هم انجام تراکنش قابلیت درخواست مشابه از میزبان را دارد. دسترسی به اطلاعات خاص کارت ها توسط موارد زیر کنترل می شوند:

- سیستم عامل داخلی کارت
- مجوزهای از پیش تعیین شده توسط صادر کننده کارت در رابطه با شرایط فایل ها. کارت می‌تواند با فاکتور استاندارد سی آر ۸۰ ، و یا در یک دانگل یو اس بی، یا سیم کارت جی اس ام باشد.

تهدید نسبت به کارت‌ها و امنیت داده‌ها

برنامه‌ریزی موثر سیستم‌های امنیتی، نیاز به کاربر مجاز برای دسترسی راحت به داده‌ها را مطرح می‌کند. در حالیکه تهدیدهای بسیاری وجود دارند که این دسترسی درستی و ایمنی اطلاعات را ارائه می‌کند. برای ایمن‌سازی همه سیستم‌های کارت صرفنظر از اندازه و نوع، مراحل اساسی وجود دارد.

تجزیه و تحلیل: ایمن سازی انواع داده ها، نقاط تماس، انتقال، خطر یا تاثیر نسبی از دست رفتن اطلاعات مهم روی کارت‌های.

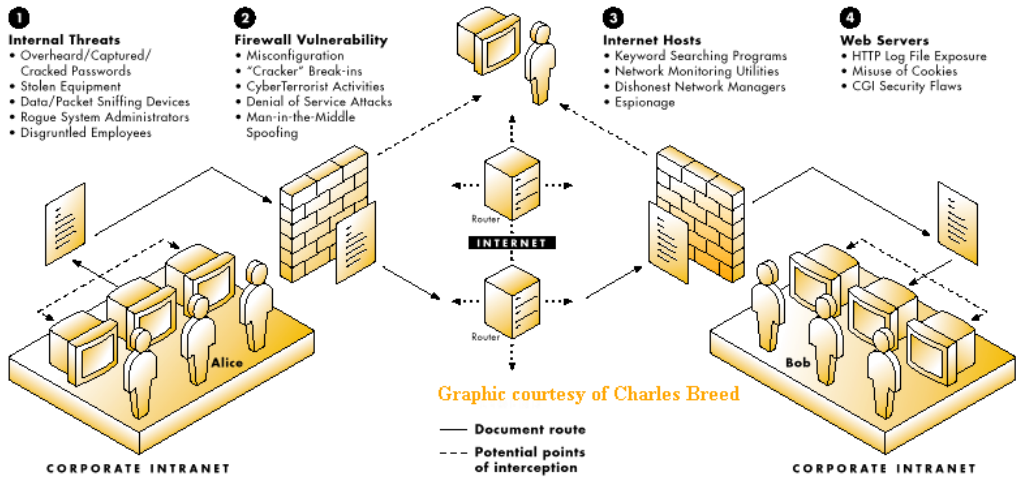
استقرار سیستم پیشنهادی

تست گذرگاه: تلاش برای هک سیستم.

حسابرسی: نظارت بر امنیت تناوبی، بررسی سیستم، میزان سازی دقیق.

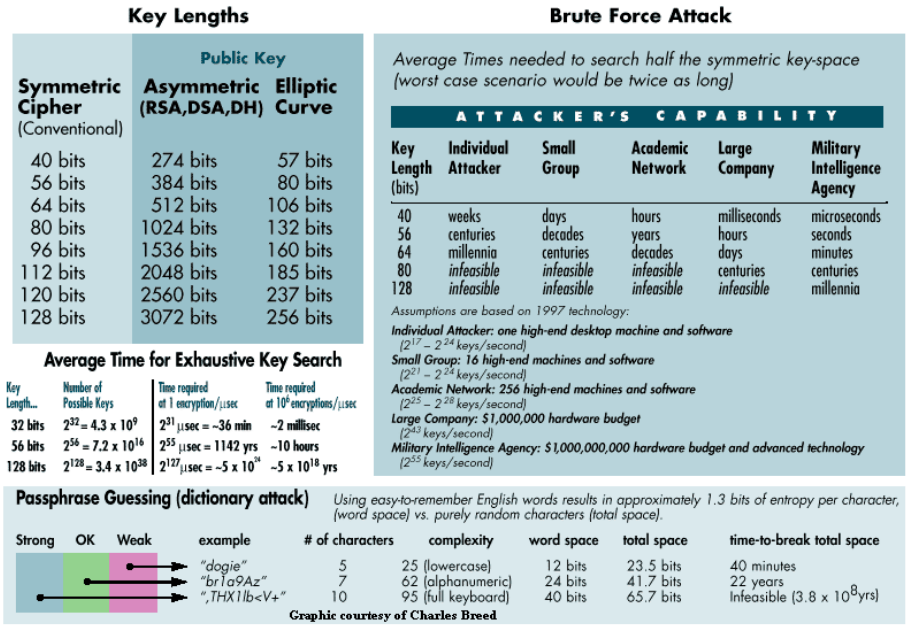
هنگام تجزیه و تحلیل تهدید به داده‌ها، یک سازمان باید توجه کافی به دو جنبه مهم داشته باشد: حملات داخلی و حملات خارجی. اولین و رایج ترین خطرکشف رمزداده‌ها از کارکنان ناراضی است. با آگاهی از این موضوع، یک مدیر خوب سیستم تمام داده‌ها یک نسخه پشتیبان را به طور مخفیانه تهیه می‌کند و آنها را در یک فضای امن قسمت‌بندی شده قرار می‌دهد. معرفی ویروس‌ها و تلاش برای فرمت کردن درایوهای شبکه، کاری رایج در مورد خطر حملات است. با بکارگیری کارت‌های کارکنان که زمان و تاریخ ورود

کارمند به سیستم و دستگاهی را که کارمند با آن مشغول کار است را ثبت می‌کند مانع از این نوع حملات می‌شود.



(شکل شماره ۱۵– امنیت گذرگاه و تست آن)

حملات خارجی بطور معمول، ضعیف‌ترین حلقه پوشش امنیتی یک شرکت را مورد هدف قرار می‌دهد. اولین مکان، یک هکر خارجی، جایی را جستجو میکند تا ببیند از کجا می‌تواند داده‌ها را مورد رهگیری قرار دهد. در یک سیستم کارت هوشمند این نقطه شروع با کارت است.



(شکل شماره ١٦ – اطلاعات کارت و کلیدهای عمومی و خصوصی)

مجموعه سوالات زیر مربوط به تجزیه و تحلیل است:

٣ آیا اطلاعات انتقال یافته روی کارت، واضح یا رمزگذاری شده است؟

٤ اگر رمز کشف شود، آیا هر جلسه با کلیدی متفاوت ایمن سازی شده است؟

٥ آیا داده‌ها از کارت به طور واضح به کارت‌خوان کامپیوتر شخصی وارد شده است؟

٦ آیا کامپیوتر شخصی یا مشتری داده‌ها را واضح انتقال داده اند؟

٧ آیا بسته کشف شده هر جلسه با کلیدی متفاوت ایمن‌سازی شده است؟

٨ آیا سیستم عامل دارای یک نسخه پشتیبان است؟

٩ آیا یک سیستم مکانیزه برای آپلود و دانلود عملکرد کد وجود دارد؟

١٠ ایمنی سیستم چقدر است؟

١١ آیا سازنده کارت، اقدامات احتیاطی را در محل برای تامین امنیت داده‌ها را انجام داده است؟

١٢ آیا آنها تعهدات را درک می‌کنند؟

۱۳ آیا آنها قادرند اقدامات امنیتی دیگری که روی کارت یا ماژول اجرا می‌شود برای کارت فراهم کنند؟

۱٤ وقتی کارت در معرض حملات دیفرانسیل قدرت و دیفرانسیل حرارتی است آیا سیستم عامل اسرار را فاش می‌کند؟

مشکلات دیگری که تهدیدی برای دارایی محسوب می شوند به قرار زیر هستند:

- کلمه عبوری که بدرستی ایمن نشده
- پین های تعیین شده و مکانیزم‌های جایگزین
- خدمات احراز هویت
- تقسیم بندی ضعیف داده ها
- امنیت فیزیکی (حذف فیزیکی یا تخریب سخت افزار)

معماری امنیت

هنگام طراحی یک سیستم، یک برنامه‌ریز، باید در هزینه‌های کل مالکیت دقت داشته باشد. این هزینه‌ها شامل:

- تجزیه و تحلیل
- نصب و راه اندازی و استقرار
- خدمات واگذار شده
- آموزش
- مدیریت
- ممیزی و ارتقاء
- هزینه های زیر ساخت (نرم‌افزار و سخت‌افزار)

بیش از ۹۹ درصد از تمام شبکه‌های مالی آمریکا بر اساس زیرساخت کلید مخفی ایمن شده اند. این تغییر در طول زمان طبق حجم خالص تراکنش هایی که روزانه مدیریت می شوند و مشکلات موجود در مدیریت کلید مخفی بوجود آمده است. سیستم‌های کلید مبنا مخفی معقول بنظر می‌رسند در صورتی که کاربر مبنا از ۵۰۰ هزار شرکت کننده کمتر باشد. سیستم کلید عمومی، معمولاً در حجم‌های بزرگ مقرون به صرفه است جایی که اعتبار داده‌ها زیاد است آنقدری که ارزش دارد هزینه بیشتری نیز صرف می‌شود. آنچه را که بیشتر مردم درک نمی‌کنند این است که سیستم‌های کلید عمومی برای انتقال داده‌ها هنوز به شدت وابسته به رمزنگاری با استفاده از کلید مخفی هستند. الگوریتم رمزنگاری کلید عمومی، فقط برای طرد نشده‌ها و برای تضمین تمامیت داده‌ها استفاده می‌شود. زیرساخت‌های کلید عمومی به عنوان یک قاعده مکانیزم امنیت داده‌ها را در یک جایگاه متناسب بکار می‌گیرد و اطمینان حاصل می‌کند که امنیت در بالاترین سطح وجود داشته باشد.

PKI چیست؟

PKI یا Public Key Infrastructure عبارتست از تکنولوژی، فرایند و خط مشی که محیطی را برای تآمین امنیت بر اساس شناسایی، محرمانه بودن، امانت داری، انکار ناپذیری و کنترل دسترسی فراهم می‌سازد.

PKI این امکان را به مردم و تجار می‌دهد که از نرم‌افزارها و ابزارهای امن اینترنتی بهره ببرند. این سیستم به بازرگانان اجازه می‌دهد از اینترنت استفاده کرده تا اطلاعات مهم تجاری آنان از رهگیری، دخالت و دسترسی غیر مجاز در امان بماند. به عنوان مثال ترکیب قانونی و امن ایمیل و تبادلات مالی تحت اینترنت و انتقال خدمات تماماً در سایه PKI تحقق می‌یابد.

PKI کاربران را قادر می‌سازد از یک شبکه عمومی ناامن مانند اینترنت به صورتی امن و خصوصی برای تبادلات اطلاعات استفاده کنند. این کار از طریق یک جفت کلید رمز عمومی و اختصاصی که از یک منبع مسؤل و مورد اعتماد صادر شده و به اشتراک گذارده می شود انجام گیرد.

این سیستم مجموعه ای است از استانداردها، فناوری‌ها و روال‌هایی که برای معتبر سازی و انتقال داده‌ها بکار گرفته می شوند. با استفاده از کلیدهای دیجیتالی عمومی و اختصاصی به منظور رمزنگاری و رمزگشایی، همچنین با استفاده از گواهینامه‌های دیجیتالی که حاوی کلیدهای اعتباری و عمومی کاربر بوده و اعتبار و هویت کاربر را اعلام می‌کنند امکان انتقال امن داده‌های الکترونیکی را فراهم می‌آورد.

وقتی دو نفر بخواهند با هم ارتباط برقرار کنند، فرستنده اطلاعات، از کلید عمومی مربوط به دریافت کننده اطلاعات برای رمزکردن اطلاعات استفاده کرده، آن را ارسال می کند. سپس دریافت کننده از کلید خصوصی خودش برای رمزگشایی اطلاعات و خواندن آن استفاده می کند. از آنجا که این کلید، خصوصی است و برای کس دیگر قابل دسترس نیست فقط آن کسی که اطلاعات برای او ارسال گردیده می تواند آن را بخواند.

PKI شامل ۲ عامل اصلی است: کلید عمومی رمزنگاری و گواهینامه اعتبار.

پنهان سازی و آشکار سازی

فایده های PKI در استفاده از کلید عمومی رمزگذاری مشخص می شود. اساسی ترین ثمره کلید عمومی رمزگذاری همان پنهان سازی (رمزگذاری) و آشکارسازی (رمزگشایی) اطلاعات دیجیتالی می‌باشد.

رمزگذاری تبدیل اطلاعات به صورت اطلاعات اتفاقی و نامفهوم می‌باشد. حالت بدون معنای آن، آن را از محفوظ ماندن اطلاعات رمزگذاری شده حتی افراد غیر مجاز به آنها دسترسی پیدا کنند، مطمئن می‌سازد.

تنها راه جهت تبدیل اطلاعات به صورت قابل فهم انجام عملیات عکس عملیات رمزگذاری است که با نام آشکارسازی (رمزگشایی) معروف است. رمزگذاری عمومی شامل پنهان سازی و آشکارسازی به وسیله کلیدهای عمومی و خصوصی انجام می‌گیرد.

کلیدهای عمومی و کلیدهای خصوصی

کلیدهای عمومی و خصوصی هر دو از دو کلید رمزگذاری مرتبط و مجزا (معمولا رشته بلندی از اعداد) تشکیل شده اند.در زیر نمونه ایی از کلید عمومی را مشاهده می کنید.

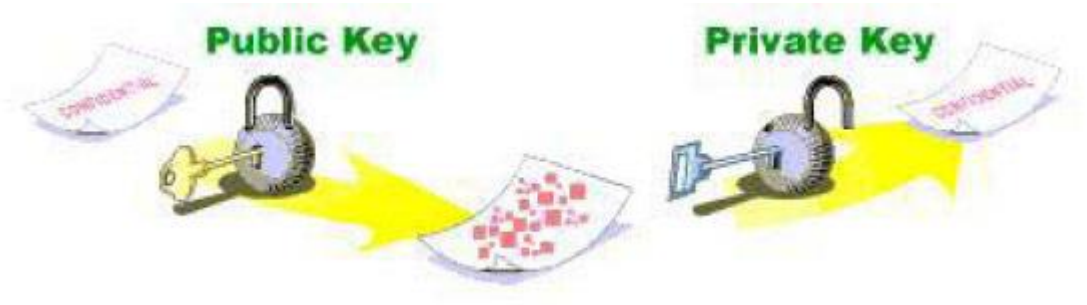
C9 18FA CF8D EB2D EFD5 FD37 89B9 E069

کلید عمومی کلیدی است که در اختیار تمام کسانی که از یک منبع خاص یا فهرست مشخص استفاده می‌کنند قرار دارد. در حالیکه کلید خصوص بایستی به صورت محرمانه نزد دارندگان مجاز آن باقی بماند.

(شکل شماره ۱۷ – کلید عمومی و خصوصی)

چون هر دو کلید به صورت محاسباتی به هم مربوط می باشند، هر چیزی که با یک کلید عمومی رمزگذاری می‌شود تنها با کلید خصوصی مربوط به آن قابل رمزگشایی است و بالعکس.

به عنوان مثال اگر **باب** بخواهد اطلاعات محرمانه ای را برای **آلیس** ارسال کند و می‌خواهد مطمئن باشد که تنها آلیس قابلیت دسترسی و خواندن آن را داشته باشد او می تواند با کلید عمومی آلیس آنرا رمزگذاری کند. تنها آلیس به کلید خصوصی مربوطه خودش دسترسی دارد در نتیجه تنها شخصی که قابلیت رمزگشایی اطلاعات رمزگذاری شده را دارد آلیس است.

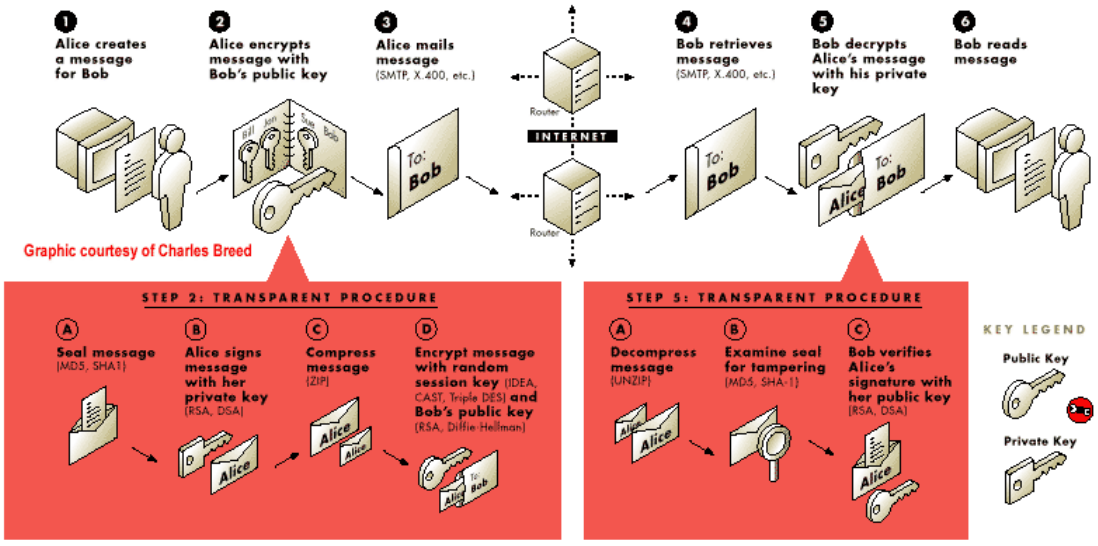


(شکل شماره ۱۸ – کلید خصوصی و عمومی PKI)

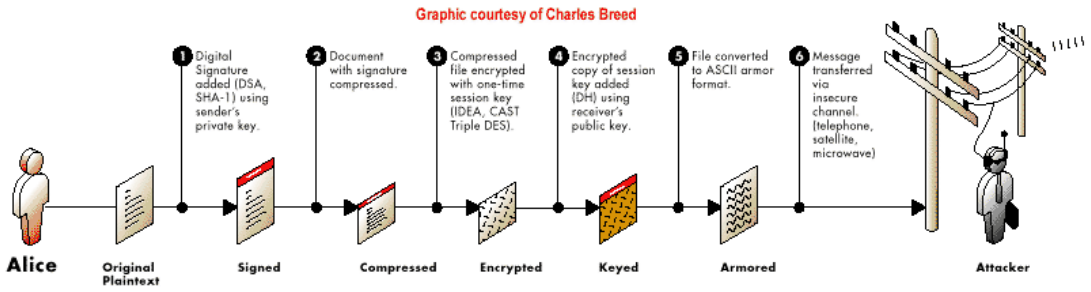
چون آلیس تنها کسی است که به کلید خصوصی خود دسترسی دارد، لذا تنها کسی است که قابلیت خواندن اطلاعات رمزگذاری شده را دارد. حتی اگر شخصی هم به اطلاعات رمزگذاری شده دسترسی پیدا کند چون به کلید خصوصی آلیس دسترسی ندارد، نمی تواند آن را بخواند.

زیرساخت PKI

تصاویر زیر سیستم PKI مبنا را نشان می‌دهند :



(شکل شماره ۱۹ – سیتم PKI)



(شکل شماره ۲۰ – امنیت در PKI)

فصل پنجم

کاربرد کارت هوشمند

کاربردهای کارت هوشمند

کارت‌های هوشمند دارای مزایا و قابلیت‌های بسیاری هستند و این باعث شده‌است تا بسیار مورد توجه قرارگیرند و کاربردهای آن‌ها بسیار گسترش یابد.

برخی از مزایای این کارت‌ها عبارتند از:

- **اندازه**: اندازه این قبیل کارت کوچک است و نیاز به حمل مدارک و پول را برطرف می‌سازد.
- **امنیت**: به دلیل وجود سیستم‌های حفاظتی روی کارت نظیر رمزنگاری، از داده‌های موجود بر روی آن به خوبی محافظت می‌شود.
- حجم اطلاعات قابل‌حمل: کارت‌های هوشمند قادرند حجم زیادتری از اطلاعات را در مقایسه با کارت‌های مغناطیسی درخود ذخیره کنند.

برخی دیگر از مزایای کارت‌های هوشمند غیرتماسی عبارتند از:

- راهکار ایده آل برای تراکنش سریع
- امکان برقراری ارتباط در فواصل
- کاربردهای عدم استفاده از دست
- طول عمر بیشتر کارت و کارت‌خوان (بدلیل عدم نیاز به تماس مستقیم بین کارت و کارت‌خوان)
- امکان سرویس به بیش از یک شخص در آن واحد
- جلوگیری از بروز مشکل در استفاده از کارت

امروزه در بسیاری ازکشورها، از کارت‌های هوشمند در کاربردهای مختلفی استفاده می‌شود، این کاربردها به طور کلی به سه دسته طبقه‌بندی می‌شوند:

- **کاربردهای شناسایی**

از این کارت‌ها برای شناسایی هویت افراد و صاحبان آنها استفاده می‌شود. مثل کارت تردد، کارت پارکینگ.

- **کاربردهای مالی**

بیشترین کاربرد کارت‌های هوشمند در زمینه پرداخت الکترونیک است. به عنوان نمونه، در کاربردهایی مانند کارت‌های نقدی و اعتباری، کیف پول الکترونیک، کارت های وفاداری (بن های سازمانی، تخفیف برای اعضاء و ...) و کارت‌های پارکینگ و بلیط. از خدمات پرداخت استفاده می‌شود. در دیگر حوزه ها نیز، خدمات این کارت ها برای کارت بهداشت و درمان، حمل و نقل، تشخیص هویت، دسترسی و ورود به مکان های خاص و ...، مورد استفاده قرار گرفته است. گستره کاربرد و سرعت فراگیری کارت های هوشمند، امروزه آن را به یکی از الزامات زندگی شهری تبدیل کرده است و به همین دلیل بسیاری از کشورها در حال سرمایه گذاری وسیع در این زمینه هستند.

در این مقاله به دلیل محدودیت، به پنج گروه اصلی از کاربردهای کارت اشاره شده و ضمن معرفی اجمالی کاربردها در هر گروه، یکی از آنها تشریح خواهد شد. این گروه های خدمات عبارتند از:

- حمل و نقل درون شهری و بین شهری
- گردشگری
- فرهنگی – رفاهی
- پرداخت شهروندان
- نیروی انسانی سازمان ها

✓ خدمات حمل و نقل درون شهری و بین شهری

در این گروه از خدمات، حداقل می توان به پانزده تنوع از کاربردهای کارت هوشمند اشاره کرد که ضمن ذکر نام آنها، یکی از خدمات حمل و نقل بطور اجمال تشریح خواهد شد. این خدمات پانزده‌گانه عبارتند از: استفاده از کارت های هوشمند بعنوان بلیط الکترونیکی در حمل و نقل مترو، بلیط الکترونیک برای اتوبوس های درون شهری، پرداخت کرایه تاکسی و آژانس، پرداخت هزینه توقف (پارک و پارکومترها)، توقف گاه های عمومی، مجوز ورود به توقف گاه های اختصاصی، رزرو مکان در توقف گاه های عمومی و اختصاصی، عوارض تردد در بزرگ راه ها، کنترل و نظارت بر رانندگان وسایط نقلیه عمومی و اختصاصی، بلیط الکترونیک برای اتوبوس های بین شهری، بلیط الکترونیک برای قطارهای مسافری، بلیط الکترونیک برای سفرهای هوایی، اخذ مستقیم جریمه یا ثبت تخلف توسط نیروی انتظامی، پرداخت هزینه های سوخت (کارت سوخت) و پرداخت هزینه های تعمیرات و نگهداری خودرو (معاینه فنی، تعمیرات، بازبینی های نوبه ای، نظافت و شستشو و...).

نمونه ای از خدمات حمل و نقل: **بلیط قطارهای مسافری**

از کارت هوشمند می‌توان به عنوان بلیط چاپی قطارهای مسافری استفاده کرد. کارت‌خوان‌های مربوط را می توان در باجه صدور بلیط و نیز در سکوهای مسافرگیری نصب کرد. در هنگام تهیه بلیط از باجه صدور بلیط (در ایستگاه یا هر آژانس مسافرتی)، مسافر ضمن پرداخت هزینه بلیط از طریق کارت، کد مجوز سوار شدن به قطار مربوطه را روی کارت خود دریافت می کند. قبل از سوار شدن به قطار در سکوی مسافرگیری، با استفاده از کارت خوان مربوطه تراکنش انجام شده و دو قبض صادر می گردد که یکی برای تحویل به مسئول مربوطه و دیگری به عنوان لاشه بلیط نزد مسافر باقی می ماند. اطلاعات تراکنش‌های انجام شده توسط کارت‌خوان‌ها، در پایان هر روز از طریق تجهیزات تخلیه اطلاعات دستی (مانند رایانه کیفی) ثبت شده و به مرکز گردآوری اطلاعات و از آنجا به

شرکت صادر کننده کارت انتقال می یابد. در صورت امکان می‌توان از طریق خط سریال، اطلاعات کارت خوان ها را در دفتر ایستگاه دریافت و سپس کار ارسال به شرکت صادرکننده کارت را انجام داد. شرکت معادل مجموع مبالغ تراکنش های انجام شده را پس از کسر کارمزد به حساب سازمان مربوطه واریز خواهد کرد. با توجه به تعداد مسافران، بسته به نوع معماری کارت می‌توان از بخش تماسی یا بدون تماس کارت استفاده کرد. تکنولوژی ارتباطی در داخل ایستگاه به صورت برخط و در ارتباط با خارج از ایستگاه به صورت برون خط خواهد بود. معمولاً این نوع پرداخت ها از طریق حساب اعتباری یا کیف پول الکترونیک انجام می پذیرد. از جمله مزایای این کاربرد می توان به موارد زیر اشاره کرد:

- حذف هزینه های چاپ، توزیع، فروش و گرد آوری بلیط های کاغذی
- تسهیل و تسریع فرایند گردآوری پول
- فراهم آوردن بستر نظارتی ارزان و قابل اطمینان
- امکان گزارش گیری سریع و آسان

✓ خدمات کارت در حوزه گردشگری

استفاده از کارت هوشمند در حوزه گردشگری، عمدتاً به منظور پرداخت هزینه مراکز خرید کالا و خدمات، شناسایی و تقویت ارتباط با مشتریان وفادار و در موارد خاص، جهت کنترل دسترسی و نظارت می‌باشد که به عنوان نمونه، به کاربرد کارت در هتل ها و مراکز اقامتی اشاره می‌گردد.

استفاده در هتل ها و مراکز اقامتی

از کارت هوشمند به عنوان ابزاری برای پرداخت هزینه و مجوز استفاده از خدمات مختلف در هتل ها می‌توان استفاده کرد. در این کاربرد می‌توان در قسمت پذیرش، رستوران، بوفه و دیگر نقاط ارائه خدمات

در هتل، کارت خوان نصب کرد. دارنده کارت در هتل می‌تواند هزینه کلیه خدمات را با استفاده از آن پرداخت نماید. مجموعه کارت‌خوان‌هایی که در بخش‌های مختلف نصب شده‌اند به طور دائم اطلاعات خود را به کامپیوتر مرکزی هتل ارسال می‌کنند. این اطلاعات به صورت روزانه به شرکت صادر کننده کارت منتقل می‌گردد. شرکت نیز معادل مجموع مبالغ تراکنش های انجام شده را پس از کسر کارمزد، به حساب فرد یا سازمان مربوط واریز می‌کند.

استفاده از سیستم کارت امکاناتی را نیز در اختیار هتل قرار می‌دهد. این سیستم امکان شناسایی مشتریان وفادار را فراهم ساخته و در مواردی که هتل تمایل به ارائه تخفیف به این مشتریان را (به طور دائم یا در دوره های خاصی از سال) داشته باشد، انجام آن را تسهیل و ساده می‌کند. همچنین درصورت تجهیز هتل، می توان از کارت برای کنترل دسترسی دارنده به امکانات معینی در هتل، بهره گرفت.

از جمله مزایای این نوع خدمات، عبارتند از:

- تسهیل و تسریع فرایند گردآوری پول
- فراهم آوردن بستر نظارتی ارزان و قابل اطمینان
- امکان گزارش گیری سریع و آسان
- امکان شناسایی و یا تعریف مشتریان وفادار
- امکان ارائه تخفیف های ویژه به مشتریان وفادار و نیز، گروه های ویژه ای از دارندگان کارت، برای خدمات معین و در اوقات معینی از سال

✓ خدمات کارت هوشمند در حوزه فرهنگی – رفاهی

از جمله این خدمات می‌توان به زمینه هایی مانند: امانت کتاب در کتابخانه ها، پرداخت در مراکز تفریحی (شهربازی، سیرک و ...)، پرداخت در موزه ها؛ باشگاه های ورزشی و استادیوم ها، فرهنگسراها، سینماها و نمایشگاه ها؛ اشاره کرد. در این بخش بعنوان نمونه به روش استفاده از کارت در سینماها اشاره می‌گردد.

✓ خدمات کارت در فرهنگ سراها، سینماها و نمایشگاه ها

از کارت هوشمند می‌توان به عنوان ابزاری برای پرداخت هزینه و کنترل تردد در مکان‌های فرهنگی نظیر فرهنگسراها، سینماها و نمایشگاه‌ها استفاده کرد. در این کاربرد لازم است در ورودی محل (یا در موارد خاص هر بخش از آن) دستگاه کارت خوان نصب شود. دارنده کارت هنگام ورود به مکان فرهنگی می‌تواند هزینه استفاده از امکانات یا بخش های مختلف آن را با استفاده از کارت پرداخت نموده و مجوز استفاده از آنها را به صورت کد مناسب روی کارت دریافت کند. هنگام استفاده از امکانات (مانند ورود به سالن نمایش در سینما یا سالن های مختلف نمایشگاه)، با انجام تراکنش، ورود فرد تأیید می‌گردد و در صورت لزوم، قبضی صادر می‌گردد که به متصدی مربوطه تحویل خواهد شد. از جمله مزایای این کاربرد می‌توان به موارد زیر اشاره کرد :

- حذف هزینه های چاپ، توزیع، فروش و گردآوری بلیط
- تسهیل و تسریع فرآیند گردآوری پول نقد
- فراهم آوردن بستر نظارتی ارزان و قابل اطمینان
- امکان گزارش گیری سریع و آسان
- امکان شناسایی و یا تعریف مشتریان وفادار
- امکان ارائه تخفیف های خاص به مشتریان وفادار و نیز گروه های ویژه ای از دارندگان برای خدمات معین و در اوقات معینی از سال

✓ خدمات کارت در حوزه پرداخت های شهروندان

پرداخت های شهروندان در قبال دریافت خدمات، هم اکنون از طریق مراجعه به بانک ها صورت می‌پذیرد. در بعضی از موارد (نظیر پرداخت قبض ها) شهروندان با مراجعه به بانک، قبض مربوطه را پرداخت می‌کنند و رسید پرداخت‌های انجام شده به سازمان مربوطه ارسال می‌گردد. در موارد دیگر، شهروند پس از مراجعه به اداره یا سازمان مربوطه، از مبلغ پرداختی مطلع شده و با مراجعه به بانک مبلغ مذکور را پرداخت می‌کند و قبض آن را به اداره یا سازمان مربوطه تحویل می‌دهد. قبض مذکور در پرونده شهروند بایگانی می‌گردد. در روش سنتی نه تنها منابعی مانند زمان، هزینه تردد، هزینه های آلودگی محیط و ...، را متحمل می‌شویم، بلکه سازمان ها همواره با مغایرت اطلاعات و شکایت شهروندان مواجه هستند.

نظیر چنین روال‌هایی در مورد شرکت‌ها و مؤسسات نیز صادق است. با استفاده از فناوری کارت، تعداد جابجایی‌ها و عملیات کاغذی کاهش یافته و گزارش‌گیری از عملیات و جستجوی سوابق مربوط به شهروندان به صورت ماشینی و با سهولت و هزینه کمتری قابل انجام است. به عنوان مثال، با ایجاد کیوسک-های خدمات شهری مجهز به کارت‌خوان، بخش قابل توجهی از خدمات شهری و پرداخت های مربوط به آنها با سریع ترین و کم هزینه ترین شیوه انجام می پذیرد. هر شهروند دارنده کارت یا هر فرد حقیقی که به نمایندگی رسمی یک شرکت یا مؤسسه کارت دریافت کرده است، می تواند از این خدمات استفاده کند. از جمله این خدمات می‌توان به مواردی همچون پرداخت عوارض شهرداری، هزینه های راهنمایی و رانندگی، ثبت احوال، قبض‌های انرژی و تلفن، هزینه‌های گذرنامه و روادید؛ هزینه‌های گمرکی، هزینه‌های بیمه و غیره اشاره کرد. فرایند پرداخت در این حوزه نیز مانند بخش قبلی می‌باشد. بنابراین از تشریح مجدد عملیات و تراکنش ها اجتناب می‌گردد.

✓ خدمات کارت در حوزه نیروی انسانی

یکی از معضلات سازمان‌ها، اعطای کمک‌های نقدی و غیرنقدی و پرداخت حقوق و مزایا به کارمندان است. در این زمینه به کارگیری کارت‌های هوشمند در قالب کارت‌های اعتباری، نقدی و کیف پول-الکترونیک، موجب ایجاد سهولت و مزایای فراوان برای سازمان و کارکنان خواهد شد.

همچنین، به کارگیری کارت‌های متعدد برای کاربردهای متفاوت، یکی دیگر از معضلات و مسائل سازمان‌ها است. عدم وجود ارتباط بین این سیستم‌ها، امکان استفاده از برخی از مزایا و امکانات را سلب کرده و بعضاً موجب ایجاد فرایندها و روال های تکراری می‌گردد. با بکارگیری فناوری کارت هوشمند چند منظوره، امکان برخورداری از کلیه مزایای فوق در قالب یک کارت، امکان پذیر خواهد بود. از جمله خدمات قابل ارائه به کارکنان از طریق کارت هوشمند عبارت است از: پرداخت حقوق و مزایای ماهیانه، کمک های غیرنقدی و پرداخت هزینه های اداری (درمان، سفر، مأموریت و...)

♦ کاربردهای نگهداری اطلاعات

دراین قبیل کارت‌ها، کد شناسایی و اندکی از اطلاعات شخصی فرد درج شده است که با ارائه به دستگاه کارت‌خوان، از این اطلاعات استفاده می‌شود. کارت‌هایی نظیر کارت گواهینامهٔ هوشمند، کارت‌های درمان، کارت‌های شناسنامه، کارت دانشجویی از این نوع محسوب می‌شود.

برخی مثال‌ها از کاربردهای کارت‌های هوشمند عبارتند از:

- کارت تلفن از نوع *تماسی*
- سیم کارت موبایل
- بانکداری

- کارت خرید
- پرداخت هزینه کانال های تلویزیونی
- حمل و نقل
- کارت‌های شناسایی

کارت‌های هوشمند چند منظوره

برای تحقق دولت الکترونیک، هر فرد نیاز به چندین کارت از انواع مذکور دارد: کارت مترو، بنزین، اتوبوس شهری، شهربازی، سلامت، شناسایی، گواهی‌نامه، گذرنامه و انواع کارتهای بانکی و... . پیش‌بینی می‌شود برای تحقق دولت الکترونیک این تعداد به بیش از پانزده کارت برای هر نفر برسد. یعنی هر فرد باید همزمان چندین کارت همراه خود داشته باشد که هر کارت توسط یک سازمان یا شرکت ارائه شده است. شهروند برای تهیه و یا اصلاح هرکدام از آنها باید به محل صدور آن رفته و هزینه‌ای جداگانه بپردازد.

این تعدد کارت مشکلاتی به همراه دارد از جمله:

- صرف هزینه جداگانه برای صدور هریک
- بالارفتن احتمال گم شدن یا سرقت کارت
- زحمت بیشتر شهروندان در حمل آنها و درنتیجه استقبال کمتر از آنها
- بالا رفتن مراجعات اداری شهروندان به ادارات و موسسات صادر کننده کارت
- سردرگمی شهروندان در به خاطر سپردن رمز هر کارت
- طرح تجمیع کارت‌های مذکور راه حلی برای حل مشکلات فوق است و علاوه برآن باعث بالا رفتن ضریب ایمنی می‌شود؛ زیرا وقتی به‌جای چندین کارت متعدد برای هرفرد دو یا سه کارت صادر شود.

- می‌توان در طراحی و ساخت آن کارت تدابیر امنیتی بیشتری در نظر گرفت تا احتمال جعل و سوءاستفاده آنها کمتر شود.
- چون تعداد کارت‌هایی که هر نفر با خود حمل می‌کند اندک است احتمال گم شدن و یا فراموش شدن رمز آنها کمتر می‌شود.

برای تجمیع و ادغام کارت‌هایی که در عصر فناوری اطلاعات هر نفر می‌تواند داشته باشد و یکی از ملزومات دولت الکترونیک است، می‌توان کارت‌هایی را که از حیث کارکرد در یک دسته قرار می‌گیرند را در هم ادغام کرد. به عنوان مثال یک کارت هوشمند چندمنظوره درکاربردهای زیر استفاده می‌شود:

- به عنوان کارت شناسایی ملی و گواهینامه رانندگی
- برای نگهداری اطلاعات گذرنامه (بدون اینکه جایگزین گذرنامه شود)
- نگهداری اطلاعات و سوابق پزشکی افراد
- پرداخت عوارض بزرگراه‌ها، هزینهٔ سیستم‌های حمل و نقل عمومی و غیره
- انجام تعاملات بانکی
- پرداخت هزینه خریدهای مختصر

قسمت هایی از تکنولوژی‌های ساخت کارت هوشمند در ایران

برخی از مراحل ساخت کارت هوشمند در کشور ما توسط برخی شرکت ها انجام می شود که عبارتند از:

۱- تهیه بدنه (پلاستیک) و ظاهر آن

۲- در بخش سخت‌افزار چیپ‌های ساده‌ای مانند چیپ کارت تلفن در ایران تولید می‌شود اما چیپ‌های پردازنده‌دار تولید نمی‌شوند.

۳- در بخش نرم‌افزار در ایران روی سیستم عامل کار نمی‌شود و کارهایی که انجام می‌شود در ارتباط با با نرم‌افزارها است مانند اپلت‌ها.

اغلب فعالیت‌هایی که شرکت‌ها در این زمینه در ایران انجام می‌دهند این است که در مرحله اول سخت‌افزار لازم را شناسایی می‌کنند و در مرحله بعد برنامه کاربردی آن کارت نوشته می‌شود و شخصی‌سازی کارت (درج آطلاعات مربوط به استفاده کننده کارت) با توجه به موارد مصرف صورت می‌گیرد.

کارت هوشمند در ایران

استفاده از کارت هوشمند در ایران نیز مانند بسیاری از کشورها رواج دارد. نمونه‌ای از این کارت‌ها که در دست مصرف یا در حال راه اندازی هستند به این شرح است:

- کارت هوشمند بانکی: بانک ملت
- کارت تلفن
- سیم کارت‌ها
- کارت مجموعه ورزشی انقلاب
- کارت مترو
- کارت سوخت
- کارت سلامت : اطلاعات پزشکی افراد ، بیمه
- کارت خودرو : گارانتی ، بیمه

فصل ششم

نتیجه گیری

نتایج

با توجه به مطالب بیان شده احساس می‌گردد که نظر به روند تکنولوژی اطلاعات درجهان و به منظور جلوگیری از عقب ماندن از این رشد، کشور ما نیز می‌بایستی خود را دراین روند سهیم کرده با کشورهای دیگر در این جهت همگام شود.

یکی از ابزارهایی که در انتقال اطلاعات مورداستفاده قرار می‌گیرد، کارتهای هوشمند است. این کارت‌ها دارای فوایدی هستند ازقبیل کاهش زمان و هزینه، انتقال بهتر و سریع‌تر اطلاعات و در کل بهبود انتقال اطلاعات. بر این اساس بایستی مسئولان محترم با درنظر داشتن شرایط مختلف، امکان استفاده از این ابزارها را در کشور فراهم آورده و راهکارهای استفاده از آن را ایجاد کنند. ما نیز به عنوان افراد این جامعه بایستی خود را در این تکنولوژی سهیم دانسته و در انتقال وپیاده سازی فرهنگ لازم و استفاده از آن، دولت را یاری کنیم تا زمان پیاده سازی چنین تکنولوژی هرچه کوتاهتر گردد.

کارتهای هوشمند امنیت هر نوع معامله را بهبود می بخشند. امکان دستکاری کاربر در ذخیره سازی و شناسایی حساب در این کارتها وجود ندارد. ثابت شده که سیستم های کارت هوشمند قابل اعتماد تر از دیگر کارتهای ماشین خوان، نظیر نوار مغناطیسی و بار کد هستند. با مطالعه بسیار ثابت شد که دوام کارتها و دستگاه های کارت خوان بیشتر از هزینه نگهداری سیستم آنها است. کارتهای هوشمند نیز اجزای حیاتی سیستم های امنیتی برای تبادل داده هستند. همه برنامه های کاربردی می توانند از ویژگی های خاص و ایمنی در قالب کارتهای هوشمند بهره مند شوند.

فهرست منابع

- Lancaster, K., 1979. Variety, Equity and Efficiency, Columbia University Press, New York.
- Lindley, R., 1997. Smart Card Innovation, University of Wollongong, Australia.
- Lundvall, B.-A., 1988. A user–producer relationships. National systems ofinnovation and internationalisation. In: Lundvall, B.-A., (Ed.), National
- Systems of Innovation: Towards a Theory of Innovation and Interactive Learning, Frances Pinter, London, p. 1988.
- Lundvall, B-A., 1992. National systems of innovation towards a theory ofinnovation and interactive learning.
- Lundvall, B-A., Johnson, B., Anderson, E.S., Dalum, B., 2002. National systems of production, innovation and competence building. Research Policy 31, 213–231.
- Malerba, F., Orsenigo, L., 1997. Technological regimes and sectoral patterns of innovative activities. Industrial and Corporate Change 6(1), 83–117.
- Malerba, F., 2002. Sectoral systems of innovation and production. Research Policy 31, 247–264.

- محمد آسیایی، علی پیروی - کارت های هوشمند – صفحه ۲۱۳ - ۱۳۸۸
- ولفنگانک رانکل - مترجم : کیوان حسنی، سلیمان محمدزاده - کارتهای هوشمند- آتی‌نگر- صفحه ۲۷۲ - ۱۳۹۰
- جورج فراری ، سوزان پو- مترجم : مجید صلصال- کارتهای هوشمند- صفحه ۳٦۸ - ۱۳۸۹

Summary

The first smart cards presented to the market about four decades ago and because of their extensive application, they have been into use in a rapid and increasing speed in many countries

A smart card is made of a physical object that a computer chip card is installed on it. The memory capacity is between 1- 64 KB bites that can be changed. On the other hand, it is capable of saving files and processing the data as well as the ability to protect the stored information , the usage of these cards in all areas of human's life in every aspect is expanded.

In this project, in addition to introducing the smart cards and reference to the history of their emergences and development, the technology of smart cards and the benefits of using these cards are going to be recounted in five areas such as: transportation, traveling, cultural, welfare, citizens' daily payments and labour services for organizations.

ISLAMIC AZAD UNIVERSITY
West Tehran Branch

B.SC Thesis

On Computer Hardware Engineering

Research Title:

Smart Cards

Supervisor:
Seyed Noorolah Valeh, Ph.D

Prepared By:
Saba Sakhaeian Haji Mohammadi

Date:
Spring 2015