دانشگاه جامع علمی کاربردی واحد استان آذربایجان غربی

مرکز علمی کاربردی سازمان مدیریت صنعتی ارومیه

جزوه درس پرداخت الکترونیک

رشته مهندسی فناوری اطلاعات

گردآوری و تنظیم

مهندس علی مصاحب طلب

کارشناس ارشد سیستم های اطلاعاتی (IS)

پرداخت الکترونیکی

- زمان شروع پرداخت الکترونیکی را می‌توان سال ۱۹۱۸ دانست، یعنی هنگامی که بانک‌های فدرال آمریکا به انتقال وجوه از طریق تلگراف می‌پرداختند
- پرداخت الکترونیکی اشکال گوناگونی دارد که می‌توان آن را به دو دسته اصلی تقسیم کرد:

❖*سیستم‌های پرداخت برای معاملات عمده فروشی*

❖*سیستم‌های پرداخت برای معاملات خرده فروشی*

تعریف
پرداخت الکترونیک

سیستم‌های پرداخت الکترونیکی

تعاریف بسیاری برای سیستم‌های پرداخت ارایه شده است؛ ولی به‌نظر می‌رسد تعریف کمیته بال (BIS) تعریفی مناسب و کاملی برای آن باشد:

«سیستم پرداخت مجموعه‌ای از ابزار، عوامل فنی، قانونی، اجتماعی است که ارزش پولی را بین پرداخت‌کننده و گیرنده وجه منتقل می‌کند.»

سیستم پرداخت را این‌گونه نیز تعریف کرده‌اند: «زیرساخت فناوری و قانونی که انتقال ارزش را بین دو طرف معامله میسر می‌سازد.»

در این تعریف ساده به دو موضوع مهم اشاره شده است: یکی زیرساخت فناوری و دیگری زیرساخت قانونی. منظور از زیرساخت فناوری، مجموعه سخت‌افزارها و نرم‌افزارها است که امکان انتقال ارزش را فراهم می‌سازد و زیرساخت قانونی مجموعه قوانین، مقررات و توافق‌نامه‌هایی هستند که از سیستم پرداخت حمایت کرده و در طرفین معامله ایجاد اطمینان و اعتماد می‌کنند.

کمیته بال یا **کمیته بازل** (Basel Committee on Banking Supervision BCBS) مرکب **است از** نمایندگان **ارشد** بانک‌های مرکزی تعدادی **از** کشورهای گروه ده **است** که **معمولا** هر سه **ماه** یک **بار توسط** بانک تسویه‌های بین‌المللی به **عنوان** دبیرخانه دائمی **آن در** شهر بازل سوئیس تشکیل می‌گردد **و** به همین دلیل به کمیته **بازل معروف شده‌است**. کمیته **بازل** دارای **قدرت** قانونی نیست، ولی اکثر کشورهای **عضو آن طور** ضمنی **موظف** به اجرای توصیه‌های **آن** هستند. [1]

توضیحاتی در رابطه با سیستم های پرداخت الکترونیک

Electronic PaymentSYSTEM

- سیستم های پرداخت بخش حیاتی زیرساخت اقتصادی و مالی یک کشور هستند. عملکرد خوب آنها در انتقال امن و به موقع وجوه مهمترین اثر آنها در عملکرد کلی نظام اقتصاد می باشد. اما سیستم های پرداخت می توانند ریسک جدی برای مشترکین داشته باشند. به این ترتیب که این سیستم ها می توانند به صورت یک کانال، مشکلات را از یک قسمت از اقتصاد به بخش های دیگر منتقل کنند. این ریسک سیستماتیک دلیل اصلی توجه و علاقه بانک های مرکزی در طراحی و اپراتوری این سیستم ها می باشد.
- یک نظام پرداخت در واقع یک سری ترتیباتی است که اجازه می دهد که استفاده کنندگان پول را انتقال دهند. در حال حاضر در بسیاری از کشورهای پیشرفته پول عبارت است از سکه و اسکناس چاپ بانک مرکزی و طلب از موسسات اعتباری به شکل سپرده.
- **برای انجام پرداخت، پرداخت کننده می بایست درخواست خود را به بانکی که پول را در اختیار دارد، بدهد. این درخواست ممکن است به صورت کاغذی باشد مثل چک و یا به صورت الکترونیکی باشد مثل کارت های پلاستیکی.**
- در مرکز هر سیستم پرداخت ترتیباتی هست که انتقال پول را بین اعضای سیستم تسهیل می کند (واسطه هایی که مستقیم به سیستم و یا به یکدیگر متصل می شوند). بنابراین سیستم های پرداخت تشکیل شده اند از تعدادی از شبکه ها که اعضا را به هم پیوند می دهد، سوئیچ ها جهت توزیع پیغام ها و قانون و رویه جهت استفاده از این زیرساخت

به عبارت دقیق تر هر سیستم پرداختی شامل:

- استانداردهای فنی توافق شده و روش های انتقال پیغام ها بین اعضا
- یک ابزار توافق شده جهت تسویه طلب های اعضا از یکدیگر (مثل حساب در بانک مرکزی)
- یک مجموعه از قوانین و رویه های اجرایی

ویژگی‌های سیستم‌های پرداخت الکترونیکی

- **امنیت درپرداخت الکترونیک:**

آیا اطلاعات مالی وشخصی را به روشی می-توان تغییردادکه مانع ازافشای آن برای گروه-های غیر مجازشود؟

- **قابلیت بررسی**

یعنی اینکه سیستم بتواندتمام جنبه- های تراکنش راثبت کندتادرصورت لزوم ازآن استفاده کرد.

- **کارایی**

انجام تراکنش باهزینهٔزمانی کم

- **قابلیت اطمینان**

آیاسیستم به قدرکافی- مستحکم است- که تراکنش-هایاپول رادرصورت قطع برق،خراب شدن سرور، خرابی-های شبکه یاورودی پیش بینی نشده ازطرف کاربران ازدست ندهد؟

- **مقیاس پذیری**

درصورت افزایش بارکاری وافزایش منابع،کارایی کم نشود.

- **قابلیت مجتمع شدن**

آیا سیستم قابلیت مجتمع شدن با سیستم حساب-داری یاپرداخت دیگررا دارد؟

- **قابلیت پذیرش**

آیاسیستم ازسوی کاربران پذیرفته خواهدشد؟

- **هزینهٔپایین**

هزینهٔانجام هرتراکنش درآن پایین باشد

- **گمنامی**

اینکه مشتری بدون نیاز به معرفی خودقادربه پرداخت باشد

عناصر اصلی سیستم پرداخت

در هر سیستم پرداخت سه عنصر اصلی وجود دارد. عنصر اول مجوز پرداخت است؛ یعنی خریدار یا فرستنده وجه، به بانک مجوز می‌دهد که پرداخت صورت گیرد. عنصر دوم تهاتر پرداخت است؛ یعنی بین بانک فرستنده و بانک گیرنده (در صورتی که دو بانک دخیل باشند) باید توافق‌نامه‌ای موجود باشد تا عملیات پرداخت از حساب فرستنده به حساب گیرنده صورت پذیرد. عنصر سوم عملیات تسویه‌حساب بین دو بانک است. این عنصر مهم‌ترین جزء سیستم‌های پرداخت الکترونیکی محسوب می‌شود. برای این منظور عموما از اتاق پایاپای خودکار (ACH) استفاده می‌شود. چنین اتاق‌های پایاپایی به‌صورت خصوصی یا دولتی توسط اکثر کشورها ایجاد شده است. به‌عنوان مثال در بعضی از کشورهای پیشرفته سیستم FEDWIRE و CHIPS و ACH وجود دارد که تمام عملیات پایاپای بانکی را به صورت الکترونیکی انجام می‌دهند.

۱-مجوز پرداخت
۲-تهاتر پرداخت
۳-عملیلت تسویه حساب

Automated Clearing House (*ACH*)

برطرف شدن یا حذف دو دِین متقابل را تا اندازه‌ای که با هم معادلند، تهاتر (Set off.adjustment automatic) نام دارد

سابقه بانکداری الکترونیکی در ایران و جهان

- سال ۱۹۹۸ را می‌توان شروع تحولات در صنعت بانکداری دانست از این تاریخ به بعد بیشتر بانکهای تجاری دنیا برای بالا بردن میزان بهره‌وری خود، به استفاده از فن‌آوری‌های پیشرفته در ارائه خدمات و تبادل اطلاعات پرداختند.
- بانکداری الکترونیک در ایران، با سالها تاخیر شروع شده است. در دهه ۱۳۶۰ کامپیوتر به نحو چشمگیری در جامعه ایرانی رسوخ یافت و از کالای لوکس و تجملی به سرعت تغییر یافته و به کالای اساسی و مورد نیاز همگانی تبدیل شد و کاربردهای ویژه و حساسی را درکار، حرفه و زندگی شخصی افراد به عهده گرفت و این مقدمه‌ای بود که بانکهای کشور نیز به فکر استفاده از این هدیه‌ی شگفتی‌آفرین تکنولوژی افتادند.
- نخستین پیشنهاد طرح جامع اتوماسیون بانکی در سال ۱۳۷۲ پیشنهاد شد و در همان سال به تصویب مجمع عمومی بانکها رسید بر اساس همین مصوبه به اجرا درآوردن این مصوبه به عهده بانک مرکزی قرار گرفت و به همین منظور شرکت خدمات انفورماتیک تاسیس و آغاز به کار کرد.
- استفاده بیش از حد از رایانه، خرید و نصب ATMدر شعب، نصب آنتن‌های VSAT، راه‌اندازی تلفن بانک و ... از دیگر اقداماتی بود که یکی پس از دیگری به تحقق پیوست و بانکداری کشور را به دو بخش الکترونیک و سنتی تقسیم کرد که اولی مبتنی بر پیام‌های الکترونیکی و دومی مبتنی بر کاغذ بود.

و در ایران ...

در حال حاضر در ایران سوییچ شتاب (شبکه تبادل اطلاعات بین بانکی) به عاملیت بانک مرکزی و توسط شرکت خدمات انفورماتیک راه‌اندازی شده است. این شبکه به بانک‌ها اجازه می‌دهد تا طبق استاندارد ISO۸۵۸۳ اطلاعات تبادل کنند. هم‌اینک سیستم ساتنا (RTGS) و پایا (ACH) نیز روی این شبکه راه‌اندازی شده است؛ در

Automated Clearing House (*ACH*)

نظام‌های پرداخت و تسویه الکترونیک وجوه در کشور طی سال‌های اخیر با معرفی طرح نظام جامع پرداخت کشور، پیشرفت‌های چشمگیری را تجربه نموده است. روند این پیشرفت‌ها به طور مشخص از سال ۱۳۸۰ قابل تشخیص می‌باشد. طرح نظام جامع پرداخت پروژه‌ای ملی است که بستر اصلی و اساسی نقل و انتقال الکترونیکی وجوه را فراهم می‌سازد. این طرح از سال ۱۳۸۰ گردآوری شد. به‌علاوه معرفی و مراحل مختلف آن با سرعت مناسبی در حال انجام است. از جمله تحولات مثبت در این زمینه می‌توان به راه‌اندازی شبکه تبادلات الکترونیک بین‌بانکی (شتاب) در سال ۱۳۸۱، سامانه حواله الکترونیک بین‌بانکی (سحاب) در سال ۱۳۸۵ و سامانه تسویه ناخالص آنی (ساتنا) در این سال اشاره نمود. علاوه بر این، اقدامات و برنامه‌های دیگری نیز در زمینه بانکداری الکترونیک و نظام‌های پرداخت در دست پیگیری است که از آن جمله می‌توان به راه‌اندازی کامل سامانهٔ پایاپای الکترونیکی (پایا)؛ راه‌اندازی سامانه تسویه اوراق بهادار الکترونیکی (تابا)؛ یکپارچه‌سازی حساب‌ها و ایجاد شناسهٔ حساب بانکی ایران (شبا)؛ ترویج بیشتر کارت‌های اعتباری و پرداخت الکترونیکی در پایانه‌های فروش و نیز پیاده‌سازی و استقرار کامل سیستم بانکداری متمرکز[1] توسط بانک‌ها اشاره نمود.

طرح نظام جامع پرداخت پروژه‌ای ملی است که بستر اصلی و اساسی نقل و انتقال الکترونیکی وجوه را فراهم می‌سازد

و در ایران...

بر اساس تعریف بانک تسویه بین‌المللی (BIS)، نظام پرداخت شامل مجموعه‌ای از ابزارها، روش‌های بانکی و نوعاً نظام‌های انتقال وجوه بین‌بانکی است که گردش پول را ممکن می‌سازند. بر اساس گزارش‌های این بانک نظام‌های پرداخت و تسویه را می‌توان به دسته‌های زیر تقسیم نمود:

انتظار می‌رود با گسترش بیشتر کارت‌های اعتباری، کارت‌های پیش پرداخته و پایانه‌های فروش در سراسر کشور و ترویج فرهنگ استفاده از آنها، بر سهم تراکنش‌ها در پایانه‌های فروش افزوده شده و نقش پول نقد در مبادلات کاهش یابد

نظام‌های پرداخت وجوه بزرگ؛ نظام‌های پرداخت وجوه خرد؛ نظام‌های تسویه و تصفیه اوراق بهادار؛ نظام‌های تسویه مبادلات خارجی و نظام‌های تصفیه و تسویه برای معاملات مشتقات[۲].

همان‌طور که گفته شد طرح نظام جامع پرداخت کشور از سال ۱۳۸۰ معرفی گردید. با پایان یافتن مراحل پیاده‌سازی اجزای طرح مزبور کلیه پرداخت‌های بین‌بانکی به صورت کاملاً الکترونیک و برخط صورت خواهد پذیرفت. طرح مزبور شامل مکانیزم‌های پشتیبانی از پرداخت‌های کلان آنی، پرداخت‌های خُرد با تعداد زیاد، نظام تسویه اوراق بهادار (اوراق مشارکت) الکترونیکی و نظام تصویربرداری از چک خواهد بود. ازاین‌رو به نظر می‌رسد اجرای کامل طرح نظام جامع پرداخت بتواند تحول و جهش عمده‌ای را در تسهیل مبادلات بانکی و اقتصادی کشور موجب شود[۳].

جدول (۱) روند گسترش ابزارها و تجهیزات پرداخت الکترونیک در کشور

مقطع زمانی	تعداد				تعداد به ازای یک میلیون نفر			
	کارت‌بانک‌ها	خودپردازها	پایانه‌های فروش	پایانه‌های شعب	کارت‌بانک‌ها	خودپردازها	پایانه‌های فروش	پایانه‌های شعب
پایان سال ۱۳۸۳	۷/۵۷۹/۷۵۷	۲/۸۶۴	۱۸/۲۳۷	۷/۵۲۲	۱۱۰/۹۰۴	۴۲	۲۶۷	۱۱۰
پایان سال ۱۳۸۴	۱۳/۵۱۱/۵۳۹	۴/۴۵۸	۶۸/۵۲۲	۱۱/۲۶۸	۱۹۴/۷۱۹	۶۴	۹۸۸	۱۶۲
پایان سال ۱۳۸۵	۲۳/۲۲۷/۶۰۱	۷/۲۶۸	۱۹۲/۷۶۵	۱۶/۶۹۲	۳۲۲/۴۶۷	۱۰۶	۲/۷۲۲	۲۲۳
پایان سال ۱۳۸۶	۳۸/۵۹۳/۲۸۳	۹/۹۱۷	۴۲۷/۰۸۲	۲۱/۷۰۷	۵۳۹/۵۲۵	۱۳۹	۵/۹۷۱	۳۰۳
پایان سال ۱۳۸۷	۶۰/۰۷۸/۲۷۱	۱۲/۹۵۹	۷۶۳/۹۲۸	۲۷/۰۴۸	۸۲۷/۷۰۷	۱۷۹	۱۰/۵۲۵	۳۷۳
پایان دی ۱۳۸۸	۸۱/۶۶۰/۷۷۳	۱۶/۱۹۶	۱/۰۷۷/۲۵۴	۳۰/۸۵۱	۱/۱۱۸/۷۵۰	۲۲۲	۱۴/۷۵۸	۴۲۳
درصد تغییر								
۱۳۸۴	۷۸/۳	۵۵/۷	۲۷۵/۸	۴۹/۸	۷۵/۶	۵۳/۳	۲۷۰/۱	۴۷/۵
۱۳۸۵	۷۳/۵	۶۷/۵	۱۸۱/۳	۳۹/۳	۷۰/۷	۶۴/۹	۱۷۶/۹	۳۷/۱
۱۳۸۶	۶۴/۷	۳۲/۸	۱۲۱/۶	۳۸/۳	۶۲/۳	۳۰/۹	۱۱۸/۳	۲۶/۳
۱۳۸۷	۵۵/۷	۳۰/۷	۷۸/۹	۲۴/۶	۵۳/۴	۲۸/۸	۷۶/۳	۲۲/۸
دهماهه اول ۱۳۸۸	۳۵/۹	۲۵/۰	۴۱/۰	۱۴/۱	۳۵/۲	۲۴/۳	۴۰/۲	۱۳/۴

جدول (۲) تعداد تراکنش‌های انجام شده در پایانه‌های الکترونیک کشور

مقطع	خودپردازها	پایانه‌های فروش	پایانه شعب	جمع
۱۳۸۶	۶۱۲/۵۷۴/۹۸۳	۳۳/۷۹۴/۲۸۳	۳۱/۹۳۷/۶۸۶	۶۷۸/۳۰۶/۹۵۲
ده ماهه اول ۱۳۸۷	۶۲۴/۹۴۰/۲۷۸	۶۳/۸۲۸/۵۲۷	۳۰/۴۹۲/۳۴۶	۷۱۹/۱۶۱/۱۵۱
۱۳۸۷	۷۹۹/۶۹۸/۴۴۵	۸۸/۸۶۱/۱۵۰	۳۹/۱۲۳/۸۰۰	۹۲۷/۶۸۳/۳۹۵
ده ماهه اول ۱۳۸۸	۱/۰۲۳/۸۶۲/۲۱۴	۱۵۵/۲۹۲/۵۹۶	۱۳۲/۰۳۷/۹۴۱	۱/۳۱۱/۱۹۲/۷۴۸
درصد تغییر				
سال ۱۳۸۷ به سال ۱۳۸۶	۳۰/۵	۱۶۲/۹	۲۲/۵	۳۶/۸
ده ماهه اول ۱۳۸۸ به دوره مشابه ۱۳۸۷	۶۳/۸	۱۴۳/۷	۳۳۳/۰	۸۲/۳
سهم از کل تراکنش‌ها				
۱۳۸۶	۹۰/۳	۵/۰	۴/۷	۱۰۰/۰
ده ماهه اول ۱۳۸۷	۸۶/۹	۸/۹	۴/۲	۱۰۰/۰
۱۳۸۷	۸۶/۲	۹/۶	۴/۲	۱۰۰/۰
ده ماهه اول ۱۳۸۸	۷۸/۱	۱۱/۸	۱۰/۱	۱۰۰/۰

شبکه شتاب در ایران

- شتاب یا شبکه تبادل اطلاعات بین بانکی یک شبکه الکترونیکی بانکی فراگیر در ایران است که توسط بانک مرکزی جمهوری اسلامی ایران در سال ۱۳۸۱ با هدف ایجاد، راه‌اندازی و راهبری سوئیچ ملی به منظور اتصال شبکه پرداخت بانک‌ها به یکدیگر و نهایتاً ایجاد زمینه برای انجام مبادلات بین بانکی به صورت الکترونیکی ایجاد شد.عضویت در مرکز مزبور تابع مقررات حاکم بر مرکز شتاب مصوب خرداد ماه ۱۳۸۱ می‌باشد.
- سوئیچ ملی در فاز اول اتصال شبکه کارت بانکها و خودپردازها و در فازهای بعدی تبادل کلیه تراکنشهای بین بانکی شامل چک‌ها، حواله‌ها و اوراق بهادار را مد نظر دارد
- هم اکنون بانک‌های اقتصاد نوین، پارسیان، پاسارگاد، پست بانک، تجارت، توسعه صادرات، رفاه کارگران، سامان، سپه، سرمایه، سینا، صادرات، صنعت و معدن، قرض‌الحسنه مهر ایران، کارآفرین، کشاورزی، مسکن، ملت, ملی،بانک دی،بانک انصار،بانک ایران زمین،بانک گردشگری،بانک حکمت ایرانیان،بانک توسعه تعاون به همراه موسسه اعتباری توسعه و بانک شهر و...در شبکه شتاب فعالند.

درانجام یک پرداخت الکترونیک حداقل ۴نقش وجوددارد:

- **پرداخت کننده**:کسی است که بابت چیزی پول پرداخت میکند.درواقع مشتری است
- **دریافت کننده**:کسی است که بابت چیزی پول دریافت میکند.درواقع فروشنده است
- **بانک کارگذارمشتری یامؤسسۀمالی صادرکنندۀ اعتباربرای مشتری**
- **بانک کارگذارفروشنده**

اجزای سیستم پرداخت

- با توجه به تعریف بانک جهانی و بانک تسویه های بین المللی(BIS) سیستم پرداخت، نظامی است که دارای اجزای زیر می باشد:
- موسسات ارایه دهنده خدمات مالی
- ابزارهای تسویه و پایاپای
- قوانین حاکم بر این سیستم

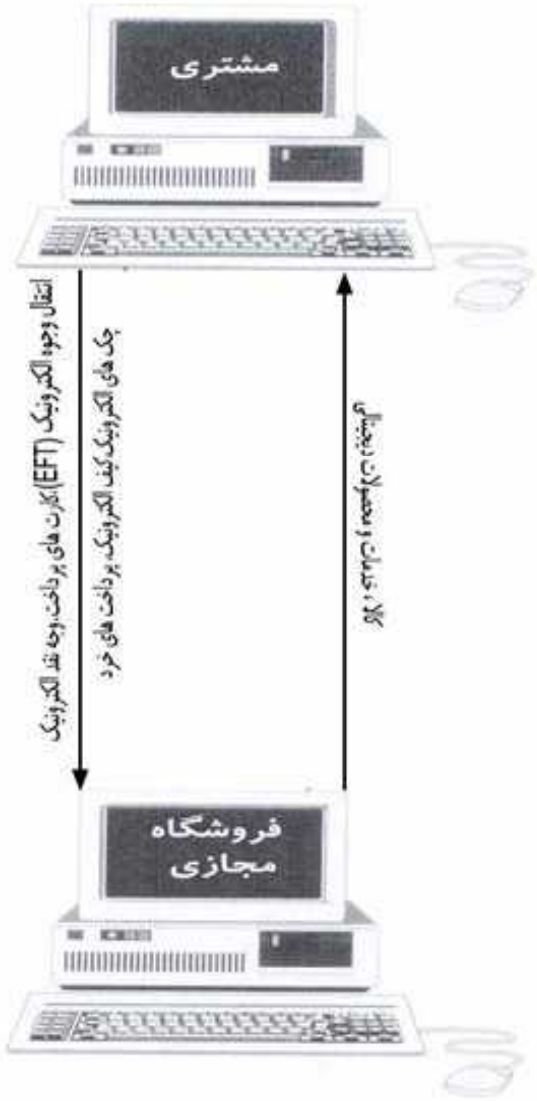
اصول سیستم های پرداخت

- ۱- سیستم باید تحت رویه های قضایی مرتبط، بر اصول حقوقی محکمی استوار باشد.
- ۲- قوانین و رویه ها باید به گونه ای باشند که تمام اعضای دیگر در آن سیستم بتوانند درک روشن و دقیقی از ریسک های مالی مشارکت در آن داشته باشند.
- ۳- سیستم باید به طور دقیق رویه های مدیریت ریسک های اعتباری و نقدینگی را تعریف و مشخص کند. این امر موجب تعیین دقیق مسئولیتهای اعضا و اپراتورهای سیستم می گردد و سبب ایجاد انگیزه مناسب جهت مدیریت و کنترل ریسک های یاد شده می گردد.
- ۴- سیستم باید بتواند به صورت به هنگام تسویه نهایی را در همان روز مبادله شده انجام دهد. ترجیحاً در طول روز و یا حداقل در انتهای روز
- ۵- سیستم باید تحت تسویه یک جانبه قادر به حصول اطمینان از تکمیل تسویه های روزانه باشد.
-

اصول سیستم های پرداخت

- ۶- دارایی هایی که جهت تسویه مورد استفاده قرار می گیرند ترجیحاً به صورت طلب از بانک مرکزی باشند، در جائیکه از سایر دارایی استفاده می شود باید ریسک اعتباری و نقدینگی نداشته باشند یا بسیار کم باشد.
- ۷- سیستم باید درجه بالایی از ایمنی و ثبات عملیاتی را تضمین کند و همچنین باید ساز و کارهایی اقتضایی جهت تکمیل پردازش روزانه داشته باشد.
- ۸- سیستم باید شکلی از پرداختها را در اختیار بگذارد که هم برای استفاده کنندگان آن عملی باشد و هم برای اقتصادی که در آن فعالیت می کند، کارایی داشته باشد.
- ۹- سیستم باید یکسری اهداف و معیارهای مشخص و در اختیار عموم داشته باشد که اجازه مشارکت آزاد و عادلانه در سیستم پرداخت را به همه افراد بدهد.
- ۱۰- ترتیبات کنترل و اداره سیستم باید موثر، قابل اتکا و آشکار برای همگان باشد.
-

-اهداف اصلی سیستم پرداخت الکترونیکEPS



- سیستم های پرداخت الکترونیک، سیستم های نرم افزاری و سخت افزاری را به گونه ای در کنار هم قرار می دهند که در نتیجه آن مشتریان را قادر می سازد به صورت (On-line) بابت محصول خریداری شده و یا خدمت ارایه شده وجه خود را پرداخت نمایند، **اهداف اصلی سیستم پرداخت الکترونیک شامل افزایش کارایی، بهبود امنیت، افزایش رفاه و آسایش مشتری و همچنین سهولت در استفاده از سیستم پرداخت می باشد.** برای پیاده سازی EPS چندین ابزار و روش وجود دارد.
- در تجارت معمول و سنتی، مشتریان بابت خرید کالاها و خدمات از وجه نقد، چک یا کارت های اعتباری استفاده می نمودند. خریداران آن لاین برای خرید کالاها و خدمات به صورت آن لاین امکان دارد که از سیستم های پرداخت که در ادامه بیان می شود استفاده نمایند:

انواع مدل های سیستم های پرداخت

- **کارت های اعتباری:** این نوع از کارت ها بر اساس اعتبار مشتری قابل شارژ بوده و یکی از رایج ترین روش های استفاده از سیستم پرداخت الکترونیک به شمار می رود.
- **پول الکترونیک:Electronic Money, e-money or e-cash .** یک وجه یا پول. استاندارد می باشد که قابلیت تبدیل به شکل الکترونیکی را دارا است و از آن می توان برای پرداخت بابت خریدهای آن لاین استفاده نمود.
- **هدایای الکترونیک: Electronic Gift**:یکی از شیوه های ارسال گواهی هدیه یا وجوه الکترونیکی از یک شخص به شخص دیگر می باشد. دریافت کننده هدیه مزبور قادر است در فروشگاه ها و مغازه هایی که چنین هدیه ای را قبول می نمایند، به خرید بپردازند.
- پرداخت قبوض آب، برق و تلفن ماهیانه به صورت آن لاین

انواع مدل های سیستم های پرداخت

- **کارت های هوشمند-Smart Card .** در این نوع از کـارت هـا ارزش مشخصی ذخیره شده و علاوه بـر آن اطلاعـات شخصـی و مالی مهمی در آن گنجانده شده است که از آن برای پرداخت آن لاین استفاده می گردد.
- **کیــف الکترونیــک:Electronic Wallet** کیـف الکترونیکـی شبیه کارت های هوشمند می باشد و در آن میـزان مشخصـی از پول ذخیره شده است.
- **سیستم های پرداخت خرد یا کوچک Micropayment . System** که شبیه کیف های الکترونیک می باشد شـامل میـزان مشخصی از پول است که در آن ذخیره گردیـده اسـت امـا از آن برای پرداخت های کوچک استفاده می گردد.

کارت های پرداخت

- مناسب ترین ابزار برای موارد پرداخت به صورت الکترونیک، کارت های پرداخت می باشد و شامل موارد ذیل می باشد:

❖ کارت های اعتباری Credit Cards

❖ کارت های بدهی Debit Cards

❖ کارت های شارژی – قابل شارژ Charge Cards

❖ کارت های هوشمند Smart Cards

Credit Cards =کارت اعتباری

- از جمله مهم ترین ابزار این کار است که اعتبار آن توسط بانک یا موسسه صادرکننده تعیین می شود و حتی اگر دارنده کارت در حسابش پولی نداشته باشد نیز قابل اعمال است. دارندگان این کارت ها می توانند تا سقف اعتبار تعیین شده، خرید یا پول برداشت کنند، اما باید تا زمان مشخصی (معمولا ۳ یا ۶ ماه) با موسسه صادرکننده کارت تسویه حساب کنند. به طور معمول مشتریان حدود چند درصد بهره نیز در ماه برای اعتبار خرج شده پرداخت می کنند. ثمین کارت یکی از نمونه های اولیه این نوع کارت ها در ایران بود.

قابلیت های کارت اعتباری چیست ؟

- ۱-خرید اینترنتی Electronic Purchase
۲-استفاده از دستگاههای خود پرداز .ATM
۳-استفاده در جایگاههای بنزین که مجهز به سیستم خود پرداز هستند.
۴-خرید در فروشگاهها و مراکز تجاری که مجهز به ترمینالهایی جهت ارائه کارت اعتباری و برداشت از آن به جای پرداخت پول هستند.
۶-استفاده از مزایای اعتباری.

automated teller machine

MasterCard , Visa Debit : کارت اعتباری

- در این حالت برای شما یک حساب بانکی به نام خودتان نزد یکی از بانکهای خارجی افتتاح می شود. این سرویس شامل دو کارت Visa Debitو Mastercardمی باشد که به حساب بانکی شما مرتبط است .
- خرید های آنلاین یا آفلاین از طریق این کارت ها امکان پذیر می باشد .
- شما می توانید واریز ، برداشت و انتقال پول به کارت های خود را از طریق سیستم بانکی انجام دهید .
- **کارت اعتباری Visa debitنوعی ابزار پولی و اعتباری است که جایگزین مناسبی برای حمل ارز در مسافرتهای خارجی بوده و از این نظر موجبات آسایش و فراغت خاطر دارندگان آن را در این گونه سفرها فراهم می نماید.**

- کارتهای اعتباری هم اکنون در سطح بین المللی و در اقصی نقاط جهان کاربرد وسیعی داشته و علاوه بر خرید های اینترنتی ، در کلیه مکانهایی که مجهز به سیستم پذیرش کارتهای اعتباری باشند (از جمله فروشگاهها ، هتلها ، رستورانها ، تهیه بلیط هواپیما، خرید از مراکز خرید، بازدید از پارکها، موزه ها، نمایشگاها) قابل استفاده خواهند بود .
- همچنین با داشتن این کارت می توانید پول خود را از دستگاه های خود پرداز ATMدر سراسر دنیا دریافت نمایید .
- سیستم فوق دارای سرویس Online Bankingمی باشد . شما قادر به انجام کلیه عملیات بانکی از قبیل : آمار پرداخت ها و دریافت ها – انجام حواله بانکی بصورت آنلاین- پرداخت صورتحسابها – امکان تعریف حسابهای زیر شاخه با واحد پول مورد نظر – دریافت و انتقال وجوه از حسابهای بانکی و ... خواهید بود

Debit Cards= کارت بدهی

- نوع دیگری از سیستم های پرداخت الکترونیکی است. این کارت به خودی خود اعتبار ندارد و همانند حساب جاری عمل می کند. به این معنی که دارنده آن می تواند مبلغ موجود در حسابش را از راه های گوناگون مانند دستگاه های خودپرداز یا فروشگاه های الکترونیکی خرج کند. دارندگان این نوع کارت ها می توانند پس از اتمام موجودی، با واریز وجه به حساب خود دوباره از کارت استفاده کنند. ملی کارت، سپهر کارت، مهر کارت و... از این دسته از کارت های الکترونیکی محسوب می شوند.

Smart Cards=کارت های هوشمند

- **کارت هوشمند** (که با نام‌های «کارت چیپ‌دار» یا «کارت با مدار مجتمع» هم شناخته می‌شود) کارتی است که بر روی آن مدار مجتمع نصب شده‌است. از این نوع کارت می‌توان به‌جای کارت اعتباری و کارت پول یا در سیستم‌های امنیتی کامپیوتری، سیستم‌های تشخیص هویت و بسیاری موارد دیگر استفاده کرد.
- کارت‌های هوشمند از نظر اندازه و شکل ظاهری، شبیه به کارتهای اعتباری معمولی هستند.

انواع کارت های هوشمند

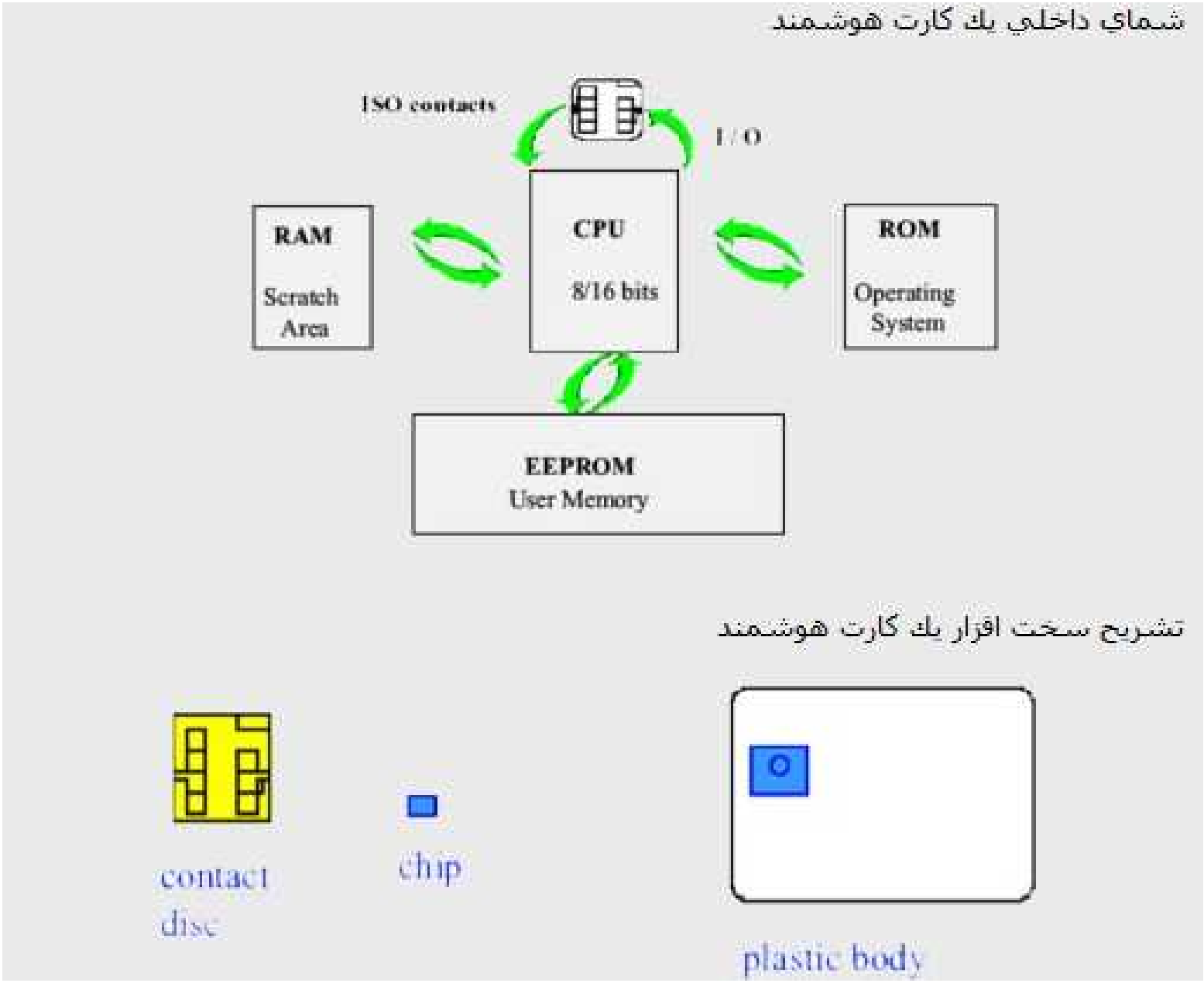
انواع کارت هوشمند ازدیدگاه کلی

- کارت هاي حافظه تماسي- Contact Memory Card
- کارت هاي داراي پردازشگر- Contact CPU Card
- کارت هاي حافظه بدون تماس- Contact-less Memory Card
- کارت هاي داراي پردازشگر با رابط دوگانه- Dual Interface CPU Card

انواع کارت هاي هوشمند از ديدگاه تکنولوژي ساخت

- کارت هاي تماسي- Contact
- کارت هاي بدون تماس- Contact-less
- کارت هاي با رابط دوگانه- Dual Interface

شمای داخلی یک کارت هوشمند



اجزای داخلی کارت هوشمند

بدنه پلاستيكي كارت : اين بدنه پلاستيكي كه در آن يك حفره مربع شكل نيز ايجاد شده است، از يكي از انواع پلاستيك هاي ذيل ساخته ميشود :

- ABS
- PVC
- PC- Polycarbonate

صفحه فلزي-Contact Disc :

كاربرد اين صفحه فلزي براي اتصال پايه هاي كوچك Chip با پايه هاي فلزي كارتخوان ميباشد و از ويژگي هاي آن ميتوان به موارد ذيل اشاره نمود:
اين صفحه فلزي هم بصورت شش پايه و هم بصورت هشت وجود دارد. از روي شكل صفحه معمولا نميتوان به نوع كارت پي برد.موقعيت اتصالات، مطابق با استاندارد 2-7816 ميباشد.

:Chip

يك Chip ، همانند ريزپردازنده يك كامپيوتر شخصي، از المان هاي سخت افزاري ذيل تشكيل شده است

- پردازشگر مركزي -CPU
- حافظه فقط خواندني- ROM
- حافظه موقت جهت نوشتن و خواندن- RAM
- حافظه دائم جهت نگهداري داده ها - از نوع E2PROM يا Flash-Memory
- درگاه سريال- Serial Port - براي ارتباط با دنياي خارج

دسته بندی بر اساس نوع تراشه به کار رفته در کارت

- **۱) کارت حافظه**
- این نوع کارت شامل واحدهای حافظه است که توسط یک سیستم امنیتی سخت افزاری محافظت می شود.
- در واحد حافظه ROM اطلاعات غیرقابل تغییر، نظیر شماره کارت و شماره دارنده کارت ذخیره می شود. از واحد حافظه EEPROM نیز برای نگهداری اطلاعاتی در طول زمان یا براساس نیاز کاربر تغییر می کنند، استفاده می شود، به عنوان مثال اطلاعات مربوط به اعتبار باقیمانده در کارت.
- از جمله کاربردهای این نوع کارت ها می توان به کارت تلفن همگانی، سیستم کنترل و شناسایی و مواردی از این قبیل اشاره کرد.
- **۲) کارت هوشمند میکرپروسسوری**
- این نوع کارت ها دارای CPU هستند و قدرت پردازش اطلاعات و انجام محاسبات را دارند.
- قیمت این کارت ها از کارت های نوع قبل بیشتر است و کاربرد آنها برای ساخت کارت های مالی، کارت های شناسایی و نظایر آن است.
- **نقش هر یک از واحدهای حافظه در این نوع کارت:**
- **ROM نگهداری سیستم عامل کارت هوشمند**
- **RAM نگهداری موقت داده ها**
- **EEPROM نگهداری برنامه کاربردی و داده های مرتبط با آن**
- **واحد واسطه- Interface** این کارت ممکن است به یکی از صورت های تماسی، غیرتماسی و یا ترکیبی باشد که وظیفه برقراری ارتباط با محیط خارج از کارت را برعهده دارد.

انواع کارتها از دیدگاه تکنولوژی ساخت

- **۱- کارت هوشمند تماسی**
- برای استفاده از این قبیل کارت‌ها، باید **اتصال فیزیکی بین کارت و دستگاه کارت‌خوان** برقرار گردد. داده‌های موجود برروی کارت به صورت سریال به کارت‌خوان ارسال می‌شود و پس از پردازش، اطلاعات جدید از طریق همان پورت به روی کارت منتقل می‌شود. به عنوان نمونه، کارت‌های تلفن عمومی جزو این دسته محسوب می‌شوند. مشکل اصلی این قبیل کارت‌ها، خراب شدن کنتاکت‌های فلزی (محل‌های تماس) بر اثر عوامل خارجی نظیر ضربه و شرایط فیزیکی محیط است.

- **۲- کارت هوشمند غیرتماسی**
- در این نوع کارت هوشمند، *ارتباط بین کارت و کارت‌خوان به‌صورت فیزیکی* بر قرار نمی‌شود؛ بلکه از طریق میدان‌های الکترومغناطیسی و یا امواج رادیویی یا RFصورت می‌گیرد. برای برقرای ارتباط، آنتن مخصوصی بین تراشه‌های کارت قرار داده شده است که در فاصله‌های کم، تا حدود ۵۰ سانتیمتر، می‌تواند ارتباط ایجاد کند. کاربرد اصلی این قبیل کارت‌ها در مواردی است که عملیات مورد نظر باید سریع انجام گیرد، به عنوان نمونه می‌توان به کارت‌های متروواشاره کرد. مزیت اصلی این قبیل کارت‌ها علاوه بر سهولت استفاده، عمر طولانی‌تر و ضریب ایمنی بالاتر آن است؛ زیرا در این نوع کارت، تراشه به همراه آنتن در میان لایه‌های تشکیل‌دهندهٔ کارت قرار می‌گیرد.
- **۳- کارت هوشمند ترکیبی(با رابط دوگانه)**
- این نوع کارت ترکیبی از کارت‌های هوشمند تماسی و غیرتماسی است که با هر دو نوع دستگاه‌های کارت‌خوان سازگار است. از این نوع کارت‌ها برای ساخت کارت‌های چندمنظوره استفاده می شود.

کاربردهای کارت هوشمند

- امروزه در بسیاری از کشورها، از کارت های هوشمند در کاربردهای مختلفی استفاده می شود، این کاربردها به طور کلی به سه دسته طبقه بندی می شوند:
- **۱) کاربردهای شناسایی:** از این کارت ها برای شناسایی هویت افراد و صاحبان آنها استفاده می شود؛ مثل کارت تردد، کارت پارکینگ.
- **۲) کاربردهای مالی**
- **۲-۱) کارت های پیش پرداخته:** این کارت ها را کاربر می خرد و با ارایه آن به دستگاه کارت خوان، به جای پرداخت پول، هزینه مورد نظر از موجودی کارت کسر می شود. مانند کارت تلفن همگانی.
- **۲-۲) کارت های بانکی:** این کارت ها را بانک ها به مشتریان خود عرضه می کنند که معرف هویت الکترونیکی مشتری نزد بانک صادرکننده است. با ارایه این کارت ها به دستگاه های خودپرداز، مشتری می تواند از خدمات بانک بهره مند شود.
- **۳) کاربردهای نگهداری اطلاعات:** در این قبیل کارت ها، کد شناسایی و اندکی از اطلاعات شخصی فرد درج شده است که با ارایه به دستگاه کارت خوان، از این اطلاعات استفاده می شود. کارت هایی نظیر کارت گواهینامه هوشمند، کارت های درمان، کارت های شناسنامه، کارت دانشجویی از این نوع محسوب می شود.

- پروژه کارت هوشمند چند منظوره دولتی مالزی

- پروژه کارت هوشمند چند منظوره دولتی مالزی، از جمله فعالیت هایی است که در چارچوب برنامه MSCاین کشور اجرا شده است. این پروژه در سال ۱۹۹۹ آغاز شد و هدف اصلی آن ارائه یک کارت هوشمند چند منظوره برای کاربردهای بخش دولتی و خصوصی بود. دولت مالزی از اواخر سال ۲۰۰۱، توزیع این کارت جدید را آغاز کرده است و به تدریج تمامی شهروندان بالای ۱۲ سال در این کشور، دارای یک کارت هوشمند چند منظوره دولتی با نام MyKadخواهند بود.
- دولت مالزی برای اجرای این پروژه با دو چالش اساسی مواجه بود: مشکلات فنی و مسأله فرهنگ سازی و آمادگی مردم برای پذیرش این نوع کارت جدید. برای غلبه بر اولین چالش، اجرای این پروژه به کنسرسیومی بین المللی از شرکت های معتبر در این زمینه سپرده شد و دستگاه های دولتی مرتبط نیز موظف به همکاری با این کنسرسیوم شدند. در زمینه فرهنگ سازی نیز دولت مالزی برنامه های آموزشی متعددی را در مورد مزایای کارت هوشمند چند منظوره تهیه کرد و از طریق رسانه های جمعی به آموزش مردم پرداخت.
- **ـ در مالزی، کارت به عنوان یک کارت هوشمند چند منظوره در کاربردهای زیر استفاده می شود:**
- **ـ به عنوان کارت شناسایی ملی و گواهینامه رانندگی.**
- **ـ برای نگهداری اطلاعات گذرنامه (بدون اینکه جایگزین گذرنامه شود).**
- **ـ نگهداری اطلاعات و سوابق پزشکی افراد.**
- **ـ پرداخت عوارض بزرگراه ها، هزینه سیستم های حمل و نقل عمومی و غیره.**
- **ـ انجام تعاملات بانکی (استفاده از دستگاه های خودپرداز یا ATM**
- **ـ پرداخت هزینه خریدها.**
- **عطا امینی، ماهنامه اطلاعات علمی**

- رفرنس:http://www.ertebatesanat.ir/?p=3845

کارت از پیش پرداخته شده یا Pre Paid

- سیستم پرداخت الکترونیکی است که:این کارت همانند **کـارت بدهی** است با این تفاوت که دیگر امکان شارژ آن وجود نـدارد. کارت های تلفن موجود در کشور یکی از این نـوع کـارت هـای الکترونیکی محسوب می شوند که نمونه های مشابه آن ها مـی توانند در خریدهای اینترنتی به کار روند.

چک الکترونیکی

- **چک الکترونیکی:** چک الکترونیکی یک ابزار نوین پرداخت است متشکل از امنیت، سرعت بوده و دارای فرآیند بازدهی تمام تراکنش‌های الکترونیکی هم‌گون و توام با زیرساخت قانونی گسترش یافته صحیح است قابلیت جای‌گزینی با چک‌های کاغذی در فرآیندهای تجاری را دارد. اولین بار چک الکترونیکی توسط خزانه‌داری ایالات متحده برای آن‌که پرداخت‌های کلان را در سطح اینترنت بسازند، به‌کار گرفته شد.

- مفهوم چک الکترونیکی طی پروژه‌ای از F S T C، شرکت سرویس‌های نوین مالی Financial Services Technology Consortiurnگسترش داده شده است. FSTCدارای تعدادی عضو است که شامل تعدادی از بانک‌های بزرگ، کارپردازان فنی امور مالی، دانشگاه‌ها و لابراتوارهای تحقیقاتی است. کار فنی بر روی پروژه چک الکترونیکی در چند مرحله انجام شد. تولید ایده‌های جدید، انجام تحقیقات اولیه، ساخت و تثبیت نمونه‌های اولیه، به قاعده در آوردن خصوصیات برای سیستم آزمایشی و اجرایی سیستم آزمایش.

ویژگی های چک الکترونیکی چیست

- یک چک الکترونیکی نسخه الکترونیکی و یا به عبارتی نسخه نمایشی چک کاغذی است.

چند ویژگی اولیه چک‌های الکترونیکی از این قرارند:

- همان اطلاعاتی را دارند که در چک‌های کاغذی موجود است.
- می‌توانند با همان ارزش و چهارچوب قانونی چک‌های کاغذی پایه‌ریزی شوند.
- قابلیت پیوند به اطلاعات نامحدود و معاوضه سریع بین سایر بخش‌ها.
- می‌توانند در هر تراکنش مشابه چک‌های کاغذی امروزی استفاده شوند.
- توسعه قابل استفاده بودن در مقایسه با چک‌های کاغذی با اضافه کردن مبلغ.

چک الکترونیکی چگونه کار می‌کند؟

- چک الکترونیکی به همان روش چک‌های کاغذی عمل می‌کند:نویسنده چک Payer، چک الکترونیکی را به کمک انواع مختلفی از دستگاه‌های الکترونیکی می‌نویسد و سپس آن را به وسیله ترمینال‌های دریافت‌کننده Payerبه بانک‌های دریافت‌کننده واگذار می‌کند.دریافت‌کننده‌های الکترونیکی، چک الکترونیکی را که نوعی اعتبار رسیده محسوب می‌شود، در قالب سپرده دریافت نموده و سپس آن را به بانک‌های پرداخت‌کننده (Payer’s banks)می‌سپارند.بانک‌های پرداخت‌کننده چک الکترونیکی را تایید نموده و حساب مرتبط با چک را شارژ می‌کنند

پول الکترونیکی

- **جامعه اروپا در پیش نویس دستورالعمل خود، پول الکترونیکی را بدین‌گونه توصیف نموده است:**
- بر روی قطعه‌ای الکترونیکی همانند تراشه کارت و یا حافظه‌کامپیوتر به صورت الکترونیکی ذخیره شده است
- به عنوان یک وسیله پرداخت برای تعهدات اشخاصی غیر از مؤسسه صادر کننده، پذیرفته شده‌است.
- بدین منظور ایجاد شده‌است که به عنوان جانشین الکترونیکی برای سکه و اسکناس در دسترس و اختیار استفاده کنندگان قرار گیرد.
- به منظور انتقال الکترونیکی وجوه و پرداخت‌های با مقدار محدود ایجاد شده‌است.

مشاور امور مصرف کنندگان آمریکا، پول الکترونیکی را به این عنوان توصیف نموده‌است :

پولی است که به صورت الکترونیکی حرکت کرده و به گردش درمی آید و می‌تواند به صورت کارت هوشمند و یا کارت‌هایی که در آن‌ها ارزش ذخیره شده، یا کیف پول الکترونیکی ارایه شود. همچنین می‌تواند در پایانه فروش استفاده شده و یا بدون دخالت هیچ شخص دیگری و مستقیماً به صورت شخص به شخص مورد استفاده قرار گیرد و نیز می‌تواند از طریق خطوط تلفن به سوی بانک‌ها و یا دیگر ارائه دهندگان خدمات یا صادرکنندگان (پول الکترونیکی) به حرکت درآمده و یا خرج شود.

انواع پول الکترونیکی

- پول الکترونیکی را به شیوه‌های مختلف تقسیم‌بندی می‌نمایند، در یکی از تقسیم‌بندی‌ها پول الکترونیکی را به دو دسته تقسیم می‌نمایند:

❑ پول الکترونیکی شناسایی شده

- این نوع پول الکترونیکی **حاوی اطلاعاتی دربارهٔ هویت مالک** آن می‌باشد که تا حدودی **مانند کارتهای اعتباری** است. این پولها دارای قابلیت ردگیری می‌باشند و هویت دارنده آن قابل شناسایی است.

❑ پول الکترونیکی غیرقابل شناسایی (بی‌نام و نشان)

- این نوع پول دیجیتالی **خصوصیت مخفی بودن هویت فرد دارنده‌اش**، را در بردارد، و از این لحاظ درست **مانند پول کاغذی سنتی** عمل می‌کند. هنگامی که پول دیجیتالی از حسابی برداشت شد بدون باقی گذاشتن هیچ اثری می‌توان آن را خرج نمود و با توجه به این نکته که هنگام ایجاد کردن پول دیجیتالی از امضاهای نامشخص استفاده می‌شود امکان پی‌گیری آن برای هیچ بانکی وجود ندارد. هر کدام از پولهای الکترونیکی فوق‌الذکر به دو دسته پول الکترونیکی پیوسته و پول الکترونیکی ناپیوسته تقسیم می‌شود.

ابزارهای پذیرش کارت

ابزارهای پذیرش کارت (Card Acceptance Device):

ابزارهای پذیرش کارت (CAD) در حقیقت به‌عنوان یک واسط بین دارنده کارت و سیستم مرکزی عمل می‌کنند.

عمده‌ترین ابزارهای پذیرش کارت عبارتند از :

۱. ATM

۲. EFT POS

۳. PIN PAD

۴. Self Services Kiosk

۵. متمرکزکننده (Concentrator):

وظیفـــه این بخش، برقراری اتصال بین نقطه تماس و ارایه ســـرویس با مرکز اصلی اســـت. با توجه به بعد مســـافت و هزینه‌های مخابراتی برای افزایش راندمان و کاهش هزینه‌ها در هر شهر و یا مرکز استان، نقطه‌ای برای جمع آوری تماس‌ها در نظر گرفته می‌شـــود و این نقطه در یک شـــبکه عمومی گســـترده (wan) به ســـامانه مرکزی متصل هستند.

ATM=*Automated Teller Machine*

- به این معنی که با وجود راه اندازی شبکه شتاب شما فقط می توانید از دستگاه های ATMاین بانک ها به صورت مشترک استفاده کنید و دستگاه های POSاین بانک ها که در داخل شعب قرار دارند فقط قادر به خواندن اطلاعات کارت مخصوص بانک هستند.
- POS: *Point of sale*

EFT=Electronic Funds Transfer

- یکی از قدیمی ترین سیستم های پرداخت الکترونیک، انتقال وجوه به صورت الکترونیک (EFT=Electronic Funds Transfer) می باشد و از آن برای انتقال پول از حساب یک بانک به حساب بانک دیگر به طور مستقیم استفاده می گردد که در این حالت از هیچگونه کاغذی که به طور دستی تهیه گردد، استفاده نمی شود.
- مشتریان، شرکت ها و نهادهای دولتی از EFTبرای موارد مختلف استفاده می کنند. آنچه که به نظر می رسد این است که از EFT به عنوان شیوه ای امن، قابل اعتماد و آسان برای امر تجارت استفاده می گردد. برای مثال در مواردی همچون پرداخت عوارض، هزینه ها، اقساط و حقوق بازنشستگی، سودها و عوارض دولتی مانند حق آب، برق و تلفن می توان از سپرده مستقیم استفاده نمود و از سایر انواع EFTبه کرات در مواردی همچون **پرداخت صورتحساب ها، خریدهای خرد، خریدهای اینترنتی، مدیریت خزانه** و سایر موارد استفاده می شود.

- **به طور کلی برای هر نوع انتقال وجهی که از طریق پایانه های الکترونیکی صورت گیرد از واژه EFT استفاده می گردد.**

مزایای استفاده از EFT به شرح زیر می باشد:

- **به طور کلی برای هر نوع انتقال وجهی که از طریق پایانه های الکترونیکی صورت گیرد از واژه EFT استفاده می گردد.**
- **کاهش هزینه های اداری و عملیاتی**
- **افزایش کارایی**
- **تسهیل در امر دفترداری و حسابداری**
- **افزایش و ارتقای امنیت**

پایانه های پرداخت:

POS=Point Of Sales

یکی دیگر از تجهیزات که در بانکداری الکترونیک از آن استفاده می‌شود EFTPOSمی‌باشد.

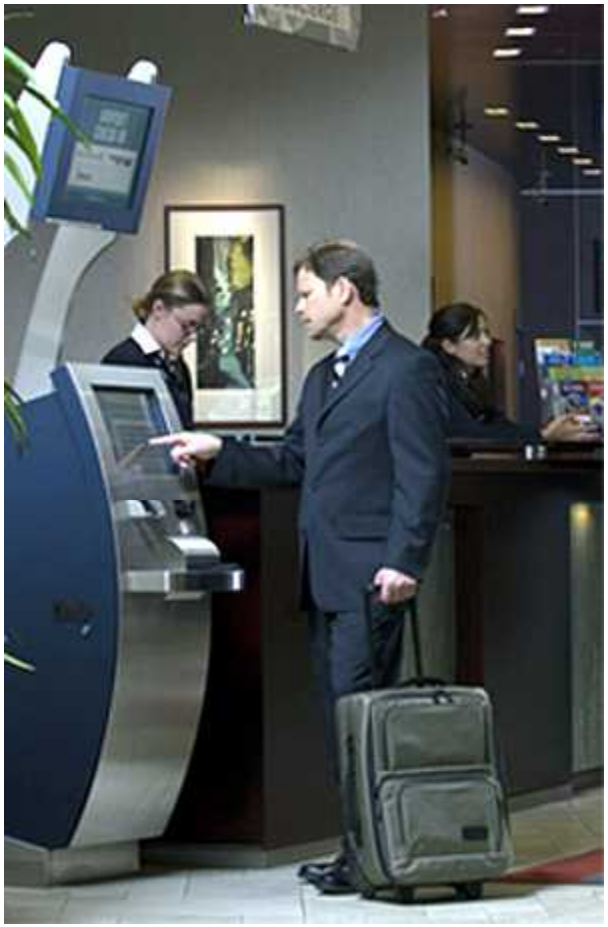
- این دستگاه نیز مانند یک رایانه شخصیPC دارای تمامی واحدهای عملیاتی از قبیل واحد ورودی، واحد خروجی، واحد پردازشگر مرکزی و واحد حافظه می‌باشد. از اینرو و بطور مستقل می‌تواند مورد استفاده قرار گیرد. این دستگاه با استفاده از مودمی که در اختیار دارد، می‌تواند از طریق خطوط تلفن به مرکز رایانه بانک یا بعبارت دیگر به «سرویس دهنده»متصل شود. این دستگاه عملیات بانکی از قبیل دریافت و پرداخت توسط کارت را انجام می‌دهد و این دستگاه نیز دارای چاپگر و دستگاه ورودی کارت خوان می‌باشد و بیشتر مواقع در فروشگاهها و سازمانهای خدماتی پذیرنده کارت مورد استفاده قرار می‌گیرند.
- دستگاه های POSپس از دریافت اطلاعات کارت مانند شماره کارت، نام دارنده و تاریخ انقضای آن، از طریق خطوط ارتباطی اعم از تلفن، اینترنت یا ماهواره با مرکز صادرکننده ارتباط برقرار می کنند و پس از بررسی وضعیت حساب کاربر، تراکنش های لازم را انجام می دهند. البته این کار به وسیله یک دستگاه کامپیوتر، دستگاه کارتخوان، اینترنت و یک کارت اعتباری امکانپذیر است.

دستگاههای Pinpad

دستگاه Pinpad مانند دستگاه EFTPOS می‌باشد با این تفاوت که‌این دستگاه مستقل از رایانه‌های شخصی (PC)قابلیت استفاده نداشته و بعنوان یکی از دستگاههای جانبی رایانه در بانکداری الکترونیک مورد استفاده قرار می‌گیرند. این دستگاه از طریق یکی از درگاهها به رایانه‌های شخصی متصل می‌شود و با توجه به رابط گرافیکی (GUI)امکان خواندن اطلاعات را از روی کارت و انجام عملیات دریافت و پرداخت بر روی حساب کارت را دارا می‌باشد.

این دستگاه در مقایسه با دستگاههای ATMو EFTPOS ارزانتر می‌باشد.

self-service kiosks



بازار هدف کیوسک های مکانیزه بسیار وسیع و گسترده است و عموم سازمان ها و مراکزی که درپی بهبود فرآیندهای اجرایی و سرویس دهی و خدمت رسانی بهتر به مراجعین و مشتریان خود با استفاده از فناوری های نوین هستند را شامل می شود. ادارات و سازمان های دولتی و حکومتی، مراکز خدماتی عمومی، بانک ها، بیمارستان ها، شهرداری ها، هتل ها، دانشگاه ها و مراکز آموزشی، فرودگاه ها، پایانه های مسافربری، فروشگاه ها، مراکز فرهنگی و ورزشی،کتابخانه ها، موزه ها، مجتمع های تجاری، کارخانجات و شرکت های بزرگ در حوزه ی بازار هدف کیوسک های مکانیزه قرار می گیرند

concentrator

چهار روش پرداخت در تجارت الکترونیک

- موفقیت تجارت الکترونیکی در چارچوب شبکه های باز، یعنی شبکه هایی است که هر خریدار جدیدی بتواند در آنها ظاهر شود. در این صورت، در حال حاضر چهار روش پیشنهاد می شود:
- -پرداخت تضمین شده توسط ثالث مورد اعتماد
- -پرداخت توسط کارت بانکی
- -پرداخت از راه دور
- -کیف پول الکترونیکی

پرداخت توسط ثالث مورد اعتماد

- این سیستم امکان پرداخت خریدهای انجام شده از طریق اینترنت را به وسیله ایمیل (مطمئن) بدون انتقال شماره کارت بانکی به فروشنده انجام می شود. خریدار و فروشنده باید از پیش در دفاتر ثبت رایانه ای ثالث مثل PayPal, PayDirect, Minutepayبا ذکر نشانی الکترونیکی و مشخصات بانکی ثبت نام کنند. سپس انتقال وجه از طریق پست الکترونیکی دارای سیستم مطمئن یا حتی به صورت خارج از خط (off-line) صورت گیرد.

پرداخت توسط کارت بانکی

- **پرداخت با کارت توسط واسط**
- در این روش یک اپراتور واسطه (مثل شرکتهای وابسته به بانکها Payment Service Provider)می تواند واسطه بین مشتری و عرضه کننده قرار گیرد و در چند ثانیه کنترل کند آیا کارت ربوده یا مفقود نشده و آیا حساب مشتری مثبت است و بانک تاجر پرداخت از طریق این کارت را می پذیرد یا خیر. این عملیات اگر توسط واسطه های مورد اعتماد صورت گیرد چند ثانیه ای بیشتر طول نمی کشد
- روش پیچیده تر این است که بانک یا موسسه مالی، خدماتی را به صورت رایگان یا در ازای وجه به مشتری پیشنهاد می کند که براساس آن شماره ای که مشتری خواهد فرستاد هر بار متفاوت باشد، مثل اینکه کارت فقط برای این یک بار به او تسلیم شده است.
- **کنترل فیزیکی(Point of Sale)**
- این شیوه انجام پرداخت توسط کارتی است که در عالم واقع با وارد کردن کارت و رمز در دستگاهی که کارت را کنترل خواهد کرد صورت می گیرد. ولی بدین منظور ضروری است که مشتری دارای دستگاه مخصوص در محل سفارش باشد. و...

پرداخت از راه دور

- در این شیوه، دستور پرداخت از **طریق موبایل یا اینترنت** به حساب فروشنده داده می شود. امنیت پرداخت از راه دور اندک است زیرا بر تراکنش های مطمئن از طریق کلمه عبور ساده استوار است.در این روش که تقریبا ترکیبی از سایر روشها با استفاده از زیرساختهای مخابراتی و اینترنتی می باشدیک شرکت ثالث نقش واسطه بین بانک و موسسات مالی با مشتریان بانکها را بر عهده می گیرد. این شرکت بوسیله عقد قرارداد با فروشندگان و عرضه کنندگان خدمات امکان پرداخت وجه توسط مشتری را برای آنها میسر می کند.

کیف پول الکترونیک virtual wallet

- در این روش، **واحدهای حساب بر روی یک قالب مادی** (کارت پرداخت که قبلا شارژ شده یا یک قالب مجازی -کیف پول مجازی virtual wallet بر روی هم انباشته می شوند و این واحدهای حساب برحسب سفارش از حساب مشتری کسر می شود.

کیف پول الکترونیک در ایران (کیپا)

- **ابزار پرداختی با قابلیت ذخیره پول الکترونیک است** که به صورت با نام و مبتنی بر فناوری های نوین ارتباطی در دو نوع پول مجازی و پول مبتنی بر تراشه صادر می شود.کاربری «کیپا» در مبادلات با مبالغ ریز بوده و وابستگی مستقیم به حساب بانکی و نیاز به ثبت در سامانه های حسابداری بانکی ندارد. همچنین پردازش الکترونیکی آن به صورت برون خطی به لحاظ اتصال به زیرساخت شبکه بانکی می باشد.
- **خدمات پرداخت الکترونیک سیار**، گستره وسیعی از فعالیت های مالی را در بر می گیرد که تحت قوانین مالی از طریق کیف پول الکترونیکی و دستگاه های قابل حمل مانند گوشی تلفن همراه ، گوشی هوشمند ، تبلت انجام می شود، **فناوری پرداخت سیار** می تواند برای انتقال پول بین افراد نیز به کار رود.

سامانه پرداخت الکترونیکی سیاردر ایران (سپاس)

- **اقدامات مدنظر جهت عملیاتی نمودن سامانه پرداخت الکترونیکی سیاردر سال ۱۳۹۲توسط بانک مرکزی بدین شرح است:**

۱- تهیه نسخه نهایی الگوی کارکردی صدور و راهبری کیف پول الکترونیک ۲(کیپا۲)

۲- تهیه نسخه نهایی مقررات و روال های ناظر بر سامانه پرداخت الکترونیکی سیار مبتنی بر کیف پول الکترونیکی

۳- تهیه نسخه نهایی مستند فنی مربوط به سامانه پرداخت الکترونیکی سیار مبتنی بر کیف پول الکترونیکی

۴- تهیه نسخه نهایی مستند امنیتی مربوط به سامانه پرداخت الکترونیکی سیار مبتنی بر کیف الکترونیکی

۵- پیاده سازی ، تست و راه اندازی سامانه پرداخت الکترونیکی سیار

http://www.cbi.ir/showitem/10555.aspx

انواع سیستم های پرداخت الکترونیکی

برخی از سیستم های پرداخت الکترونیکی که امروزه روی اینترنت استفاده و یا پیشنهاد شده‌اند، عبارتند از:

- سیستم های مبتنی بر کارت اعتباری
- سیستم های مبتنی بر چک الکترونیکی
- سیستم های مبتنی بر پول الکترونیکی
- سیستم های ریز پرداخت
- سیستم های مبتنی بر مزایده

۱) سیستم مبتنی برکارت اعتباری

همانطور که می دانید **کارت اعتباری به عنوان یکی از متداول ترین روش‌های پرداخت الکترونیکی در حال حاضر مطرح شده است،** از مهم‌ترین شرکت هایی که در زمینه کارت اعتباری فعالیت دارند می توان دو شرکت بین المللی Visaو Master Cardرا نام برد. پروتکل هایی که در این سیستم ها مورد استفاده قرار می گیرند نیز شامل SSLو SETو SEEPاست.

- پروتکل SSLیا Secure Socket Layerتوسط شرکت Netscape Communicationsبرای تدارک امنیت و محرمانگی بر روی اینترنت توسعه یافته است. **این پروتکل از تصدیق اصالت در سمت سرویس دهنده و سرویس گیرنده پشتیبانی می‌کند**. پروتکل SSLوابسته به کاربرد است و به پروتکل‌هایی نظیر HTTP، FTPو telnetاجازه می‌دهد تا به‌صورت لایه‌ای برروی آن قرار گیرند. پروتکل SSLقادر است به توافق درباره کلیدهای رمزنگاری و نیز تصدیق سرویس‌دهنده قبل از تبادل اطلاعات توسط لایه‌های بالاتر اقدام کند. پروتکل SSL، امنیت و تمامیت کانال انتقال را با استفاده از رمزکردن، تصدیق اصالت و کدهای تصدیق پیام حفظ می‌کند

۲-سیستم های مبتنی بر چک الکترونیکی

سیستم پرداختی مشابه چک است که زمانی که تراکنش انجام می شود پول ازحساب بانکی پرداخت کننده به حساب بانکی پرداخت شونده منتقل می شود.
پروتکل های این سیستم عبارتند از:

- پروتکل Netbill
- پروتکل NetCheque

۳) سیستم های مبتنی بر پول الکترونیکی

مطالعات فراوانی برای جایگزین کردن پول الکترونیکی به جای پول کاغذی صورت گرفته اما هنوز سیستم مشخصی که بتواند همه نیازها رابرآورده کند طراحی نشده است. سیستم های مرتبط عبارتند از:

- Ecash
- NetCash

۴) سیستم های ریز پرداخت

برای **انجام دادن تراکنش های کم قیمت** مانند گرفتن اطلاعات کوتاهی از یک روزنامه، گرفتن مظنه از قیمت سهام و نظایر آن از این سیستم استفاده می کنند. این سیستم به دلیل بی‌نیازی به سیستم های امنیتی و رمزنگاری (که معمولاً گران هستند) هزینه را پایین آورده و بار ترافیکی را نیز کاهش می دهد. سیستم های مرتبط عبارتند از:

- Millicent
- SubScrip
- MicroMint

۵) سیستم های مبتنی برمزایده

درسیستم های مبتنی برمزایده فرض بر این بود که طرفین تجاری از وجود یکدیگر آگاه هستند و می خواهند کالا یا وجوه خود را مبادله کنند. اما مواردی اتفاق می افتد که شرکت کنندگان زیادی در یک مبادله می خواهند دخیل باشند اما از **اهداف تجاری** یکدیگر با خبر نیستند (مانند مزایده) در این گونه موارد از سیستم مذکور استفاده می شود. سیستم مورد استفاده در این حالت X-Cashو یا پول رقمی قابل اجرا است.

اطلاعات موردنیاز جهت خرید اینترنتی چیست ؟

پرداخت اینترنتی به پرداختن پول از طریق اینترنت، در قبال دریافت کالا یا خدمات اطلاق می شود به طوری که این پرداخت بدون نیاز به حضور فیزیکی در بانک یا فروشگاه و از طریق اینترنت انجام شود. در واقع خریدار با استفاده از کارت بانکی خود می تواند از اینترنت خرید کند و پول آن را همان موقع پرداخت نماید.

اطلاعات موردنیاز جهت خرید اینترنتی چیست ؟

۱- شماره ۱۶ رقمی درج شده بر روی کارت

این شماره در کارت همه بانک ها، بر روی کارت درج شده است. نمونه شماره کارت درج شده بر روی کارت های بانک ملی در عکس زیر آمده است.

۲- رمز خرید اینترنتی یا رمز دوم

رمز خرید اینترنتی، با رمزی که شما هنگام استفاده از دستگاههای خود پرداز ATM وارد می نمائید متفاوت می باشد. حتی این رمز با رمز اینترنت بانک که حساب خود را از طریق اینترنت چک می کنید، نیز متفاوت است.

اطلاعات موردنیاز جهت خرید اینترنتی چیست ؟

کد CVV2 به صورت یک عدد ۳رقمی (و به ندرت ۴رقمی) مانند شمارهٔ ۱۶رقمی حک شده روی کارت، بر روی اکثر کارت ها حک شده است. مثلاً روی کارت های بانک های ملت، صادرات، پاسارگاد، سامان، پارسیان و... به صورت یک عدد ۳رقمی حک شده است. یا در برخی کارت های بانک ملی ۴ رقمی است و عکس آن را در زیر مشاهده می نمایید.

cvvمخفف کلمه Card Verification Valueاست که به آن کد **اعتبارسنجی** هم گفته می‌شود.

۴- تاریخ انقضاء

تاریخ انقضاء هم روی اغلب کارت های بانکی حک شده است. اگر روی کارت شما تاریخ انقضاء وجود ندارد، نگران نباشید. از عدد ۱۲ به جای ماه و از ۹۹ به جای سال انقضای کارت استفاده نمایید.

مواردی که در ارزیابی سیستم های پرداخت مهم است:

- **گمنامی:** این ویژگی **بیانگر خواسته های کاربر مبنی بر حفظ اطلاعات شخصی و خصوصی و هویت** وی می باشد.
- **قابلیت کاربرد:** ارزش افزوده مکانیزم های پرداخت به **میزان مفید بودن** این سیستم ها در خرید بستگی دارد. قابلیت کاربرد (یا مقبولیت) که در بسیاری از مراجع از این واژه استفاده نموده اند در سیستم پرداخت تا انجا تعریف مشخصی دارد که در زمان فروش آن لاین برای عمل پرداخت مناسب باشد.

- **تایید:** در ادبیات شیوه تایید **به معنای نحوه کنترل اعتبار** معامله می باشد. شیوه تایید به دو صورت آن لاین و غیر آن لاین صورت می گیرد. تایید غیر آن لاین به این معناست که کاربران در زمانیکه به شبکه وصل نمی باشند می توانند بدون حضور طرف سوم (واسطه انجام معامله) پول مورد نظر را مبادله نمایند.

- **قابلیت تبدیل**: کاربران در حالت طبیعی **از مکانیزمی استفاده** می نمایند که در زمان پرداخت بتوانند جوابگوی نیاز آنها باشد.
- **کارایی:** سیستمی که از **کارایی لازم برخوردار** باشد باید توانایی پردازش پرداخت های اندک و خرد را داشته باشد، بدون آنکه عملکرد آن متحمل کاستی و هزینه گردد (Maxemchuk and paul and Law,1994)

- **قابلیت تعامل:** در صورتیکه سیستم پرداخت تنها به یک شرکت وابسته نباشد این سیستم، یک سیستم متعامل می باشد که به سایر بخش های ذینفع نیز اجازه و امکان اتصال را می دهد. با استفاده از استانداردهای باز و جامع برای پروتکلها و زیرساخت های انتقال داده می توان به این هدف رسید.
- **چند واحد پولی:** در میان کشورهای مختلف، پرداخت های کارا و موثر، زمانی وجود خواهد داشت که سیستم های مربوط به آن **توانایی پردازش چندین واحد پولی** را داشته باشند.

مواردی که در ارزیابی سیستم های پرداخت مهم است:

- **قابلیت اعتماد:** به طور طبیعی کاربران و محیط تجاری سیستم هایی را می پذیرند که از **قابلیت اتکا و اعتماد بالایی** برخوردار باشد زیرا انجام خدمات و روال کاری واحدهای تجاری به دسترسی آسان و عملیات موفق زیرساخت های پرداخت بستگی دارد (Medvinsky and Neuman,1993,1995)

- **توانایی رشد: با** توجه به افزایش استفاده تجاری از اینترنت، **تقاضا برای استفاده از زیر ساخت های** پرداخت نیز روبه افزایش است. زیرساخت های پرداخت باید از قابلیت رشد برخوردار بوده و کاربران و فروشگاه های جدید را در خود بپذیرد. (Medvinsky and Neuman,1993)

- **امنیت:** یکی از مهمترین مواردی که در سیستم های پرداختۀ به کرات مورد بررسی قرار گرفته است، امنیت می باشد (Caum,1997)

- **قابلیت ردگیری:** قابلیت ردگیری مشخص می نماید که چگونه می توان در یک جریان پرداخت الکترونیک و خرید آن لاین، **گردش پول و منابع وجوه پرداخت شده را ردگیری** نمود.

- **اطمینان:** توجه به مواردی که در قسمت های قبل به آن اشاره شد و پیاده سازی آنها با شکل مناسب، به **جلب اعتماد و اطمینان** مطلوبی منجر خواهد شد (Wayner,2003)

- **قابلیت استفاده:** پرداخت آن لاین مساله پیچیده و مبهم نبوده و معمولاً به شیوه ای آسان و قابل اجرا صورت می گیرد الزاماتی که در مورد سیستم پرداخت الکترونیک مورد بحث قرار گرفت برای استفاده از آن می باشد

نکات امنیتی در پرداخت الکترونیکی

- رمز خود را جایی یادداشت نکنید و در صورت یادداشت نمودن، آن را در جیب یا کیف پـول بـه همراه کارت قرار ندهید.
- – رمزهای عبور خود را به صورت دوره ای تغییر دهید.
- – رمز خود را در اختیار سایر افراد قرار ندهید.
- – اطلاعات حساس از جمله رمز خود را از طریق تلفن برای دیگران بازگو نکنید.
- – در صورت فاش شدن رمز خود، در کوتاهترین زمان ممکن آن را عوض نمایید.
- – کارت و رمز خود را به هیچ وجه در اختیار دیگران قرار ندهید. بعضاً افراد سـود جـو بـه بهانـه کمک کردن و راهنمایی ضمن اخذ کارت و رمز شما پس از انجام عملیات، کارت شما را با کارت دیگری (سرقتی ، مفقودی ، باطله و...) معاوضه نموده و حساب شما را مورد سـوء اسـتفاده قـرار می دهند.
- – در صورت انجام انتقال وجه و عملیات اینترنتی برروی حسـاب خـود در مرورگرهـای اینترنـت گزینـه ی بـه خاطرسـپردن رمـز را انتخـاب نکنیـد. ایـن گزینـه بـا نـام کلـی Remember Passwordشناخته می شود، از این قابلیت استفاده نکنید.
- – برای ارسال اطلاعات حساس خود از پست الکترونیکی استفاده ننمایید.
- – همواره سعی کنید برای ورود رمز خود از امکان Virtual Keyboardبجای کیبورد فیزیکـی کامپیوتر استفاده کنید. این امکان در سیستم عامـل ویـنـدوز و همچنـین در برخـی از سـایتهای پرداخت آنلاین وجود دارد.

نکات امنیتی در پرداخت الکترونیکی

- – شناسه عبور و رمز خود را بر روی کامپیوترهای خارج از اختیار و کنترل خود وارد نکنید.
- – هنگام ورود به وب سایتها به ویژه وب سایتهایی که در آن اطلاعات محرمانه وارد می گردد، آدرس سایت مورد بازدید را در کادر نوار آدرس کنترل نمایید. بسیاری از کلاهبردارهای اینترنتی بواسطه استفاده از سایتهای جعلی و مشابه، جهت دریافت اطلاعات حساس کابران رخ می دهد.
- – در صفحاتی که سایت مورد بازدید از شما درخواست ورود شماره کارت، رمز کارت، رمز دوم و CVV2می نماید، حتماً مطمئن شوید که از پروتکل SSL استفاده شده است. بدین منظور آدرس صفحه می بایست با عبارت httpsبجای httpآغاز گردد.
- – همواره از نرم افزارهای آنتی ویروس معتبر و بروزشده استفاده نمایید.
- – سیستم عامل کامپیوتر خود را همواره بروزرسانی کرده و آخرین وصله های امنیتی را دریافت نمایید.
- –

نکات امنیتی در پرداخت الکترونیکی

- در صورتی که احتمال وجود برنامه هـای مخـرب را بـر روی کـامپیوتر خود می دهید از انجام هرگونه تراکنش مالی آنلاین خودداری نمایید.
- – پس از انجام کار مورد نیاز در وب سایتهایی که نیاز به رمز ورود دارند، به طور کامل Log outکنید.
- – به مطالب نوشته شده در پنجره هایی که اتوماتیک نمـایش داده مـی شوند توجه نموده و بلافاصله بر روی Okیا Yesکلیک نکنید. بسیاری از برنامه های مخرب بـه همـین شـیوه بـر روی کامپیوترهـا نصـب مـی گردند.
- – ایمیلهای دریافتی از منابع ناشناس را باز نکنید. به لینکهای ارائه شده در ایمیلها اعتماد نکنید، به عنوان نمونه بانکها و موسسات اعتباری هیچ گاه از طریق نامه های الکترونیکی اطلاعات محرمانه شـما را درخواسـت نمی کنند. بنابراین هرگاه در صندوق پستی خود نامه هایی از این دست را مشاهده کردید به سرعت آن را حذف کنید. از داده های حساس خود نسخه پشتیبان تهیه نموده و در جایی امن نگهداری کنید.

SSL - Secure Soket Layer

روشی است برای بر قراری یک ارتباط امن بین فروشنده و خریدار و اکنون به عنوان یک استاندارد امنیتی اینترنت شناخته شده است

SSLچگونه اتصال امن را بین دو سوکت اجاد می کند .

۱- امکان مذاکره و توافق پارامترها بین سرویس دهنده و مشتری
۲- احراز هویت سرویس دهنده و مشتری بطور مستقل و مجزا
۳- مخابره سری و رمزنگاری شده داده ها
۴- مراقبت صحت و سلامت داده ها

SSL=Secure Sockets Layer

SSL یک تکنولوژیی برای ارسال امن اطلاعات در اینترنت می‌باشد و به‌عنوان استاندارد جهانی به منظور تصدیق صحت وب سایتها و کدگذاری ارتباطات بین مرورگرهای کاربران و وب سرورها می‌باشد. گواهینامه سرورها توسط CA ها صادر می‌شود. CA ها از متدهایی برای تضمین هویت گواهینامه کاربران استفاده می کند لذا نیاز به دو تابع ضروری برای گسترش تجارت الکترونیکی امن دارند:

۱. تصدیق سرور SSL: گواهینامه سرور به کاربران اجازه می‌دهد که هویت یک وب سرور را تایید کند. مرورگرهای وب به طور خودکار گواهینامه و شناسه عمومی سرور را که از CA صادر شده است بررسی می کند.
۲. کدگذاری SSL: این گواهینامه یک کانال امن را گسترش می‌دهند تا همه اطلاعات فرستاده شده بین یک وب سرور و مرورگر وب کدگذاری شود و جلوی تداخل به این اطلاعات توسط گروه سوم گرفته شود.

Certificate Authentication

SET (Secure Electronic Transaction)

روشی است برای حفظ امنیت تراکنش های کارت های اعتباری بروی اینترنت

SETاز رمزنگاری برای رسیدن به اهداف زیر استفاده می کند :

۱- محرمانگی کار کردن اطلاعات
۲- تأمین درستی پرداخت
۳- تصدیق اصالت فروشگاه ها و دارندگان کارت اعتباری

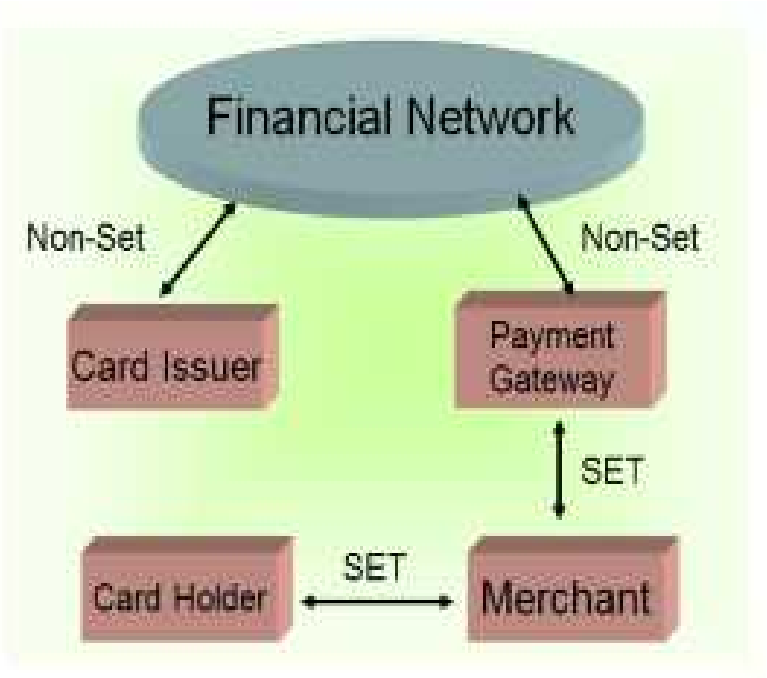
این روش علاوه برآنکه اطلاعات را رمز کرده , صحت ادعا طرفین را به یکدیگر ثابت می کند دارای یک امتیاز به روش SSLمی باشد . **در روش SETفروشنده هیچ دسترسی به اطلاعات کارت اعتباری خریدار نخواهد داشت** به عبارت دیگر اطلاعات کارت اعتباری خریدار به هنگام خرید به حساب فروشنده ارسال نشده بلکه بین خریدار و خود بانک مبادله می شود در حال حاضر SSLبخاطر ارزان تر و ساده تر بودن , بیشتر از روش SETمرود استفاده است

ادامه-مطالعه-SET

پروتکل SET (Secure Electronic Transaction): توسط ویزا و مسترکارد طراحی شد. برای امن کردن تراکنش‌های کارت اعتباری طراحی شده است. همه پیامها رمز می‌شود پس دارای محرمانگی است. همه دارای گواهی دیجیتال هستند پس اعتماد را فراهم می‌کند و می‌توان از هویت بانک اطمینان داشته باشیم. می‌توان مطمئن شد که فروشنده همانی است مد نظر ما است و خود فروشنده و بانک نیز می‌توانند مشتری را احراز هویت کنند. در زمینه Privacy اطلاعات را فقط در اختیار افرادی که به اطلاعاتی نیاز دارند قرار می‌دهد.

- Cardholder
- Merchant
- Issuer صادر کننده کارت
- Acquirer سرویس پرداخت را برای فروشنده فراهم می‌کند
- Payment Gateway رابطی است بین فروشنده و شبکه‌های مربوط به کارت اعتباری
- Certification authority

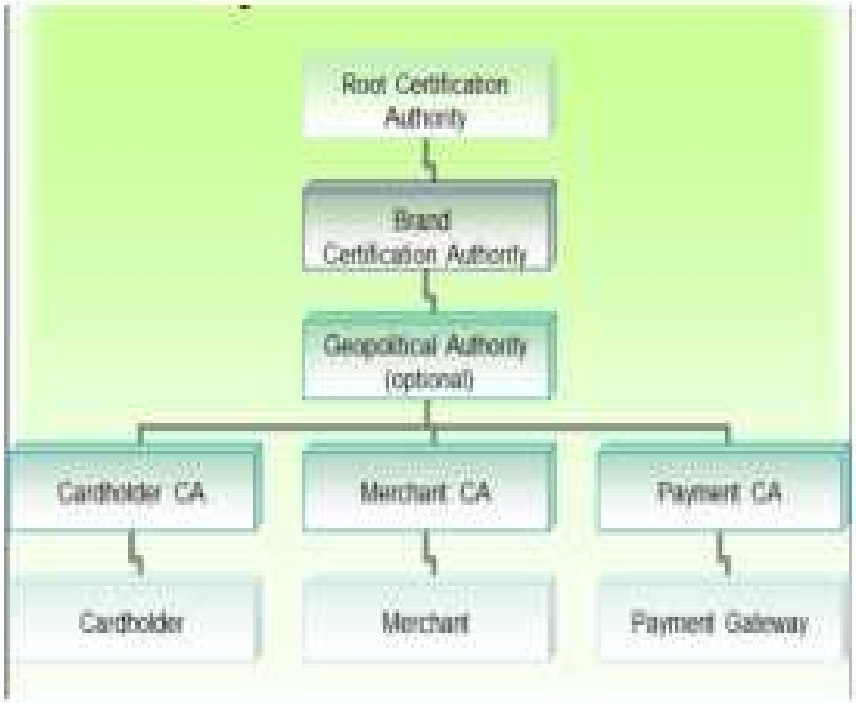
ادامه-SET



پروتکل SET ارتباط بین صاحب کارت و فروشنده و همچنین ارتباط بین فروشنده و رابط پرداخت کارت اعتباری است. بخش‌های دیگر از پروتکل‌ها Non-SET استفاده می‌کنند. از پروتکل‌های سنتی خود استفاده می‌کنند. شبکه‌های مستر و ویزا همه شرکت‌هایی که کارت را صادر می‌کنند به آن‌ها وصل می‌شوند.

ادامه-SET

وقتی مشتری می‌خواهد خرید انجام دهد و فروشنده بخواهد با رابط پرداخت ارتباط متصل شود از پروتکل SET استفاده می‌شود که از SSL امن‌تر است. مدل اعتمادی که SET استفاده می‌کند، در SET فرض شده است که همه دارای کلید عمومی هستند. این کلید باید توسط یک سازمان ثالثی تایید شود. در اینجا منظور همان مراکز صدور گواهی است که باید کلید عمومی امضا و تایید شده را صادر کنند و این گواهی بر اساس استاندارد X.509 هستند.



ادامه-SET

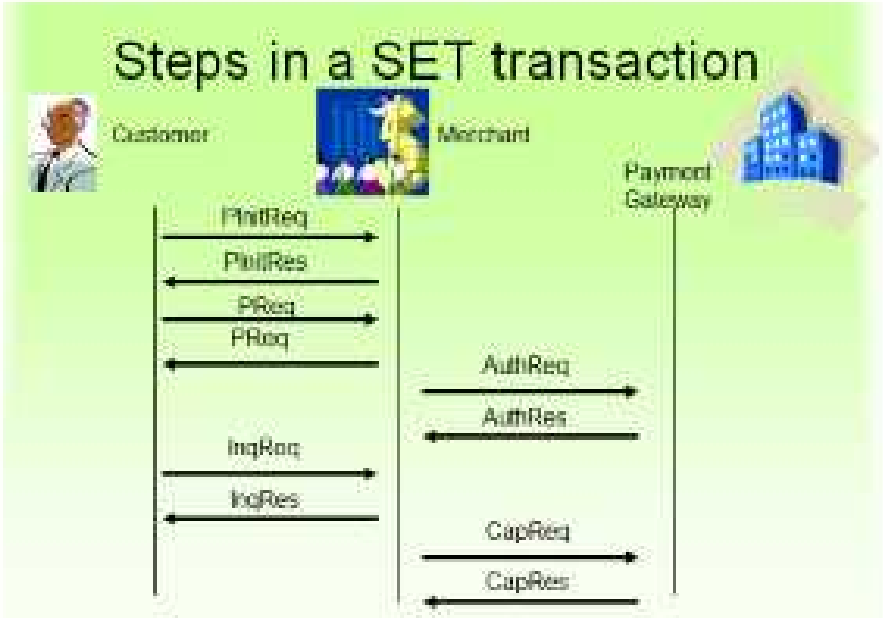
- Root Certificate Authority: مرکز صدور گواهی ریشه است و مراکز صدور گواهی میانی را احراز هویت می‌کند.
- Brand Certificate Authority: همانند مستر کارد و ویزا کارد است.
- Geopolitical Authority: که به صورت اختیاری است و مراکز صدور گواهی بر اساس موقعیت جغرافیایی است.
- Cardholder CA: برای صاحب کارت گواهی صادر می‌کند.
- Merchant CA: برای فروشنده گواهی صادر می‌کند.
- Payment CA: برای درگاههای پرداخت گواهی صادر می‌کند.

در گواهی دیجیتال یک فیلدی به نام فیلد توسعه یافته (Extention Filed) وجود دارد. فیلدی است که محدودیت برای استفاده از کلید تعریف می‌شود. مثلاً کلید برای رمز، تاییده احراز هویت استفاده شود.

SET-ادامه

پیغام‌های پروتکل SET به صورت زوج پیغام هستند.

- Initialization (PInitReq/PInitRes);
- Purchase order (PReq/PRes);
- Authorization (AuthReq/AuthRes);
- Capture of payment (CapReq/CapRes);
- Cardholder inquiry (InqReq/InqRes) [optional].



مفاهیم تکمیلی امنیت در پرداخت الکترونیک و رمزگذاری ها

ایجاد یک تجارت الکترونیکی منوط به پیاده‌سازی زیرساختارهای کامل آن می‌باشد. پرداخت اینترنتی یکی از این زیرساختارها می‌باشد که عملکرد آن از دودیدگاه مورد بررسی قرار می گیرد:

۱. بخش مشتری[۴]

۲. بخش ارئه‌دهنده‌خدمات[۵](فروشنده و بانک)

در بخش اول مشتری خواهان ایجاد یک ارتباط امن با ارائه‌دهنده خدمات است. این ارتباط بر دو اصل زیر بناشده‌است:

- در هویت ارائه‌دهنده خدمات شک و تردیدی وجود نداشته‌باشد.
- امکان استراق‌سمع در حین تراکنش برای گروه سوم وجود نداشته باشد.

در بخش دوم موارد زیر دارای ارزش خاصی است که ارائه‌دهنده خدمات در معماری سیستم خودباید به آنها بها دهد:

- در انجام تراکنشها از هویت مشتری خود اطمینان داشته باشد.
- از اطلاعات موجود بر روی شبکه کاری خود حفاظت کند.
- عملیات تراکنش مالی مشتری را انجام دهد.
- مشتری را از نتایج عملیات آگاه سازد.

بررسی امنیت در پرداخت اینترنتی

- **۴ روش تشخیص سایت های اصلی از سایت های کلاهبردار:**
- **۱-اطمینان حاصل کنید که سرور سایتی که در آن هستید در داخل ایران است:**
- استفاده از سایت هایی که برای این منظور وجود دارند: سایت هـای بیشـماری در اینترنت وجود دارند که در صورت وارد کردن آدرس یک سایت مکان سـرور آن را مشخص می نمایند. برای این منظور می توانید از سایت زیر استفاده نمایید:
- http://www.ip-adress.com/ip_tracer/178.145.1.4

- استفاده از افزونه های مرورگرها : مرورگرهایی مانند Chromeو Firefoxبرای این منظور افزونه های بسیاری دارند که با نصب آنها بر روی مرورگر مکان سرور سایت جاری نمایش داده می شود.

- افزونه IP Location Information 4.0برای مرورگر Firefox
- و افزونه Site Geo IP Locatorبرای مرورگر Chrome

بررسی امنیت در پرداخت اینترنتی

- **۴ روش تشخیص سایت های اصلی از سایت های کلاهبردار:**
- **۲-اطمینان حاصل کنید که سایت از پروتکل SSLاستفاده می کند:**
- برای تشخیص سایت های کلاهبردار کافیست به آدرس صفحه‌ای که در آن اطلاعات کارت بانکی شما خواسته می شود، توجه نمایید. چنانچه آدرس نوشته شده در نوار آدرس دروازه پرداخت اینترنتی مجهز به پروتکل SSL باشد، به عبارتی چنانچه با " https "شروع شده باشد می توان تا حدود زیادی مطمئن بود که آن صفحه یک صفحه امن بوده و متعلق به بانک مورد نظر شما است.
- جهت اطمینان، زمانی که به سایت مورد نظر وارد شدید، پس از بارگذاری کامل صفحه توسط مرورگر به ابتدای آدرس آن توجه کنید. در این حالت شما باید به جای حروف" **http"** ، حروف " **https"**را مشاهده نمایید. حرف **s**در انتهای حروف **http**، مخفف کلمه ی **Secure**به معنی ایمن می باشد.

بررسی امنیت در پرداخت اینترنتی

- **۴ روش تشخیص سایت های اصلی از سایت های کلاهبردار:**
- **۳-آدرس های اصلی دروازه های پرداخت بانک ها**
- زمانیکه در دروازه‌ی پرداخت الکترونیکی بانک مورد نظر قرار می‌گیرید، یکی از مطمئن ترین راه ها جهت اطمینان از ایمن بودن پرداخت، مطابقت دادن آدرس بالای صفحه با آدرس های اصلی دروازه های پرداخت بانکها که در زیر مشاهده می فرمایید می باشد. آدرس صفحه پرداخت شما باید با این آدرس ها آغاز گردد :

بانک ملی:
https://epayment.bmi.ir

بانک ملت:
https://pgw.bpm.bankmellat.ir/

بانک تجارت:
https://pg.tejaratbank.net/

بانک پارسیان:
https://www.pecco24.com/

بانک سامان:
https://mci.sb24.com

بانک سینا :
https://www.esinabank.com

بررسی امنیت در پرداخت اینترنتی

- **۴ روش تشخیص سایت های اصلی از سایت های کلاهبردار:**
- **۴- از معتبر بودن گواهی امنیتی صفحه اطمینان حاصل کنید.**

گواهی امنیتی صفحه ارتباط شما با بانک را رمزنگاری کرده و مانع از شنود اطلاعات شخصی شما توسط افراد مهاجم و کلاهبردار می شود. در هنگام ورود به دروازه پرداخت بانکها، قبل از درج هرگونه اطلاعات، به گواهی دیجیتالی **SSL**بانک توجه کنید. مشاهده‌ی این گواهی و اطمینان از صحت آن، بسته به مرورگری که از آن استفاده می کنید متفاوت می باشد.

- **دقت داشته باشید** که دریافت گواهینامه ی امنیت، کار بسیار سختی نیست و تقریباً همه ی افراد می توانند آن را دریافت کنند و **نکته ی حائز اهمیت، معتبر بودن این گواهینامه ها** می باشد.

- در هنگام استفاده از سایت هایی که حتی از پروتکل **SSL ("https")**استفاده می نمایند نیز باید به معتبر بودن این گواهینامه های امنیت دقت نمود، **بنابراین** به **پیغام های ظاهر شده** بر روی مرورگر خود دقت کنید.

- ترجیحا از مرورگرهای chromeو یا Firefoxاستفاده نمایید و مرورگر خود را همواره به روز نمایید. چنانچه یک گواهی دیجیتالی جعل گردد در صورت به روز نبودن مرورگر امکان عدم شناسایی جعلی بودن آن توسط مرورگر وجود دارد.

بررسی این که آیا سایت از اتصالی امن SSLاستفاده می‌کند یا نه

- اگر اطلاعات حساس شخصی را در صفحه‌ای وارد می‌کنید، در نوار آدرس به دنبال نماد قفل در سمت راست نشانی اینترنتی سایت بگردید تا ببینید آیا سایت از SSL استفاده می‌کند یا نه. SSLپروتکلی است که تونل رمزگذاری شده‌ای بین رایانه شما و سایتی که مشاهده می‌کنید، برقرار می‌کند.
- سایت‌ها می‌توانند از SSLبرای جلوگیری از مداخله اشخاص ثالث در اطلاعات انتقال یافته از طریق تونل استفاده کنند.

نماد	معنای آن
	این سایت از SSL استفاده نمی‌کند. این نماد برای سایت‌های http:// نمایش داده می‌شود. اکثر سایت‌ها به استفاده از SSL نیاز ندارند چون با اطلاعات حساس سر و کار ندارند. از وارد کردن اطلاعات حساس مانند اطلاعات کارت اعتباری‌تان یا اطلاعات ورود به سیستم بانکی‌تان در این صفحه اجتناب کنید. اگر اطلاعات حساس در سایتی که از SSL استفاده نمی‌کند، درخواست شد؛ تمام یا مالک وب‌سایت را مد نظر قرار دهید.
https://	Google Chrome **باطور موفقیت‌آمیز اتصال امنی با این سایت برقرار کرده است** اگر باید به سایت وارد شوید یا اطلاعات حساسی را در صفحه وارد کنید، این نماد را جستجو کنید و مطمئن شوید که نشانی اینترنتی از دامنه صحیحی برخوردار است. اگر سایتی از گواهی SSL تأیید اعتبار پیشرفته (EV-SSL) استفاده کند، نام سازمان نیز در کنار نماد به صورت نوشتار سبز نشان داده می‌شود.
https://	**این سایت از SSL استفاده می‌کند، اما Google Chrome محتوای ناامنی در این صفحه شناسایی کرده است.** اگر اطلاعات حساسی را در این صفحه وارد می‌کنید، مراقب باشید. محتوای ناامن می‌تواند راه نفوذی برای کسی که قصد تغییر ظاهر این صفحه را دارد فراهم کند.
https://	**این سایت از SSL استفاده می‌کند، اما Google Chrome یا محتوای ناامن با خطر بالا در این سایت شناسایی کرده است یا مشکلی در رابطه با گواهی سایت تشخیص داده است.** اطلاعات حساس را در این صفحه وارد نکنید. گواهی نامعتبر یا سایر مشکلات جدی https بیانگر این هستند که شخصی سعی دارد در اتصال شما با سایت مداخله کند.

ssl و پیام های هشدار

پیام‌های هشدار SSL

وقتی Chrome تشخیص می‌دهد سایتی که بازدید می‌کنید احتمال دارد برای رایانه شما مضر باشد، ممکن است پیام هشداری دریافت کنید.

پیام هشدار	معنای آن
احتمالاً این سایتی نیست که شما به دنبال آن هستید!	این پیام هنگامی ظاهر می‌شود که نشانی اینترنتی فهرست شده در گواهی سایت با نشانی اینترنتی واقعی سایت همخوانی نداشته باشد. ممکن است سایتی که می‌خواهید بازدید کنید، وانمود کند که سایت دیگری است. درباره این هشدار بیشتر بدانید
گواهی امنیتی این سایت قابل اعتماد نیست!	این پیام وقتی ظاهر می‌شود که گواهی توسط سازمان شخص ثالث شناخته شده‌ای صادر نشده است. چون هر کسی می‌تواند گواهی ایجاد کند، Google Chrome بررسی می‌کند که گواهی یک سایت از سازمان قابل اطمینانی صادر شده باشد. درباره این هشدار بیشتر بیاموزید
گواهی امنیتی سایت منقضی شده است! یا **گواهی امنیتی سرور هنوز معتبر نیست!**	این پیام‌ها در صورتی ظاهر می‌شوند که گواهی به روز نباشد. بنابراین، Google Chrome نمی‌تواند تأیید کند که سایت مورد نظر سایت امنی است.
گواهی امنیتی سرور باطل شده است!	این پیام وقتی ظاهر می‌شود که سازمان شخص ثالثی که گواهی سایت را صادر کرده است، این گواهی را به عنوان نامعتبر علامتگذاری کرده است. بنابراین، Google Chrome نمی‌تواند تأیید کند که سایت مورد نظر سایت امنی است.

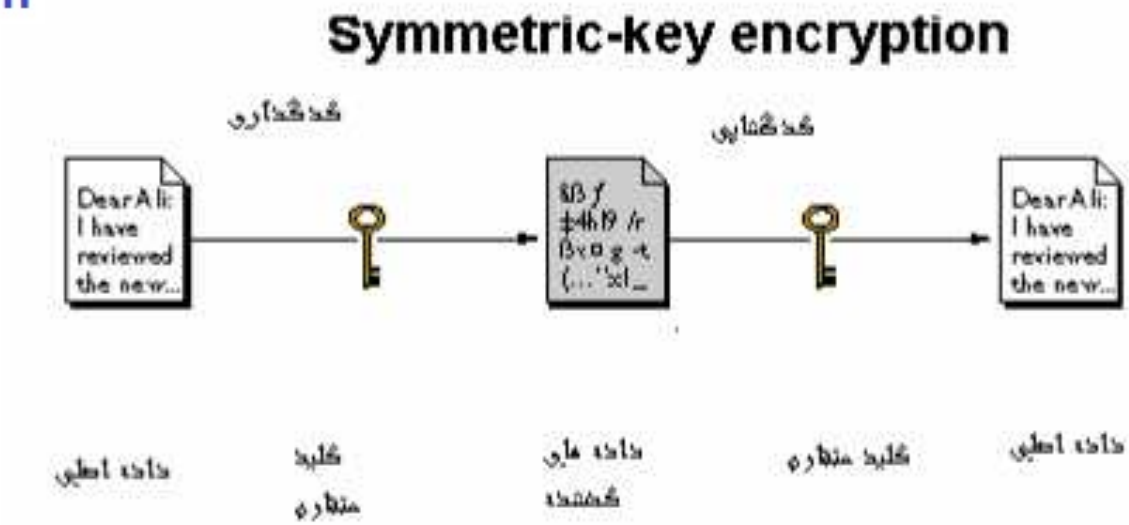
Encryption=کدگذاری

Decryption=کد گشایی

به فرایندی که موجب تغییر شکل اطلاعات می‌گردد به طوری که این اطلاعات برای همه بی‌مفهوم ولی برای گیرنده نهایی از طریق کدگشایی قابل فهم باشد، کدگذاری گویند.[۲]

به عمل عکس کدگذاری که اطلاعات تغییر شکل یافته توسط گیرنده نهایی قابل فهم باشد، کدگشایی می‌گویند.[۳]

در کدگذاری از یک تابع ریاضی با نام الگوریتم Cryptographic یا Cipher و از یک سری اعداد با نام کلید استفاده می‌کند.



رمزگذاری متقارن

در رمزگذاری پنج جزء وجود دارند:

۱- متن اصلی Plaintext

۲- الگوریتم رمزگذاری Encryption algorithm

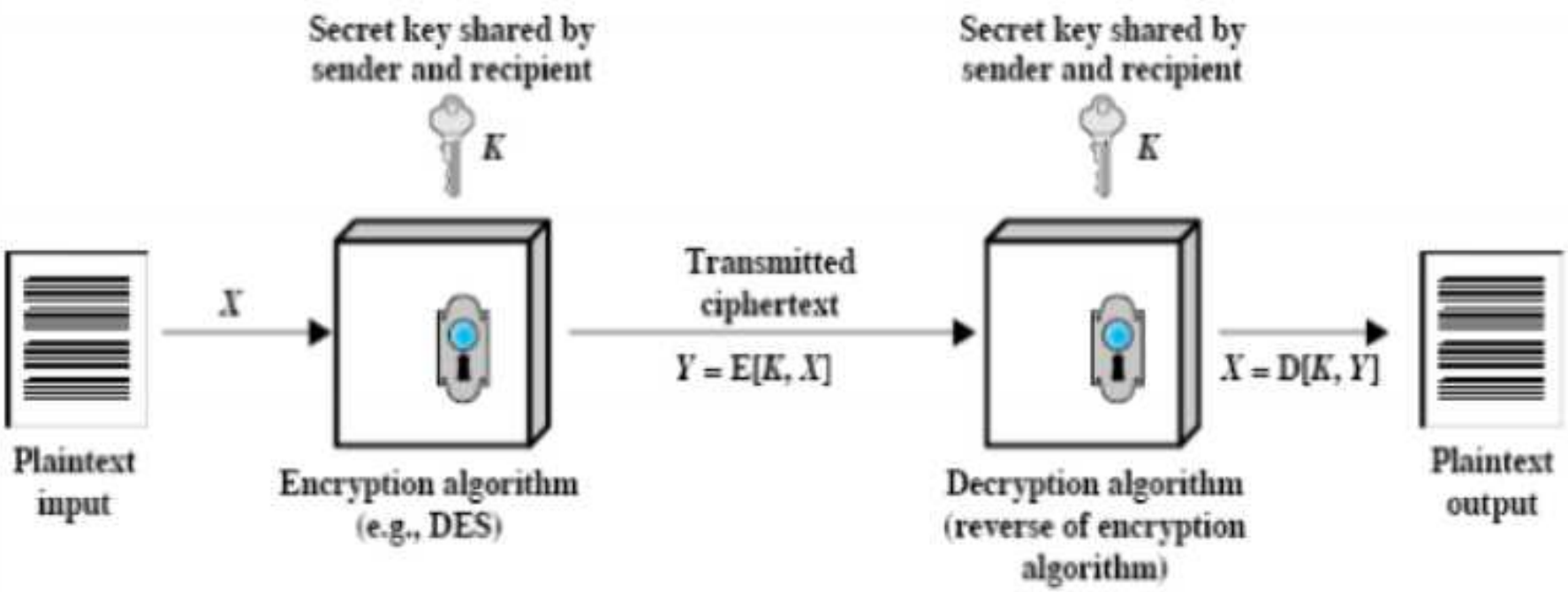
۳- کلید مخفی Secret key

۴- متن رمز Ciphertext

۵- الگوریتم رمزگشایی Decryption algorithm

امنیت رمزگذاری باید مبتنی بر کلید باشد و الگوریتم باید آشکار باشد

مدل ساده رمزگذاری متقارن



دسته بندی روش های رمزگذاری

روش‌های رمزگذاری از سه بعد مختلف دسته‌بندی می‌شوند:

۱- نوع عملیاتی که برای تبدیل متن اصلی به متن رمزی انجام می‌شود

الف- جانشینی Substitution

ب- جایگشتی یا جا به جایی Transposition

۲- تعداد کلید مورد استفاده

الف – متقارن (یک کلید) Symmetric (single key)

ب- نامتقارن (دو کلید یا رمزگذاری با کلید عمومی)

Asymmetric (two-keys, or public-key encryption)

۳- روشی که متن اصلی پردازش می‌شود

الف- رمز قالبی Block cipher

ب- رمز دنباله‌ای Stream cipher

دسته بندی الگوریتم های رمزگذاری متقارن

- الگوریتم‌های رمزگذاری متقارن

۱- استاندارد رمزگذاری داده

Data Encryption Standard (DES)

۲- DES سه تائی

Triple DES (3DES)

۳- استاندارد پیشرفته رمزگذاری

Advanced Encryption Standard (AES)

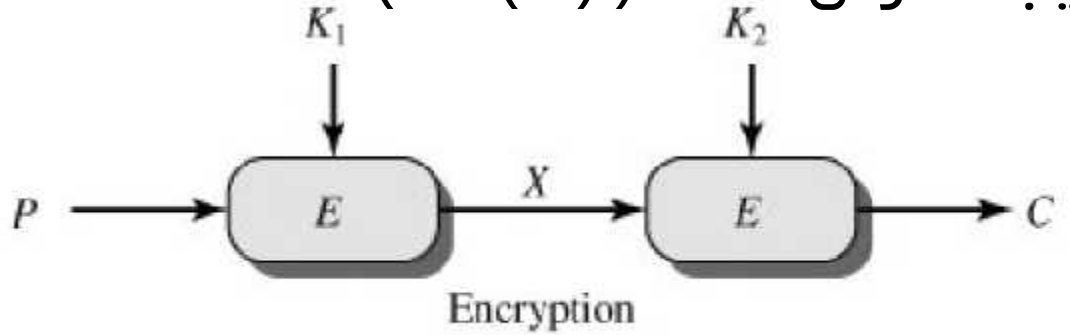
استاندارد رمزگذاری داده

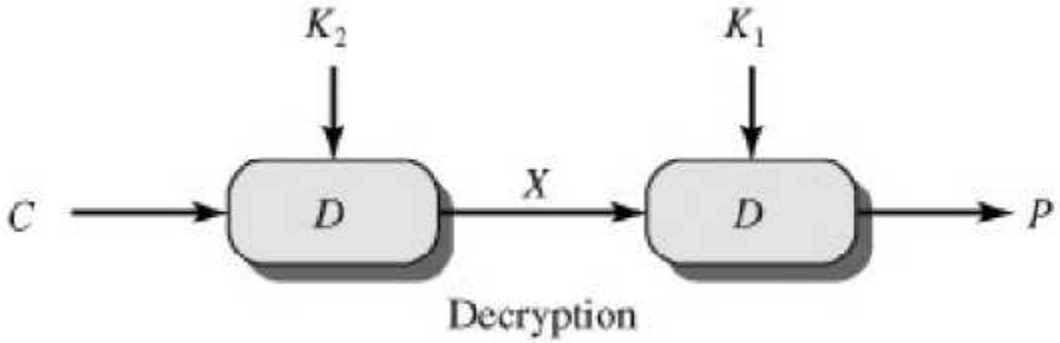
Data Encryption Standard (DES)

- پرکاربردترین روش رمزگذاری
- به آن الگوریتم رمزگذاری داده نیز گفته می‌شود
- DES یک رمز قالبی است
- متن اصلی بصورت قالب‌های ۶۴ بیتی است
- طول کلید ۵۶ بیت است

DES دوتایی (double DES)

- هر بلوک داده را دو بار با الگوریتم DES رمزگذاری کنیم.
  - استفاده از دو کلید
  - $C = E_{K2}(E_{K1}(P))$
  - رمزگشایی آن نیز به ترتیب معکوس است: $P = D_{K1}(D_{K2}(C))$

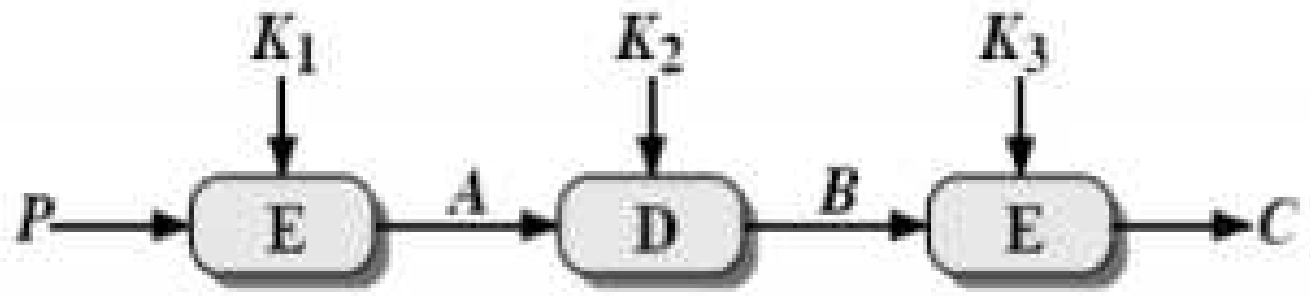




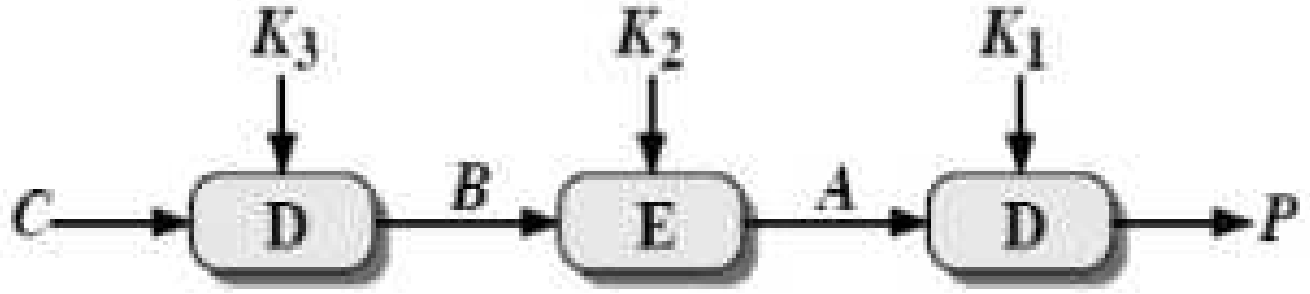
DES سه تایی (triple-DES) با دو کلید

- استفاده از سه بار رمزگذاری DES با سه کلید
  - هزینه حمله متن اولیه معلوم، به اندازه 2^112 است.
  - سرعت اجرا نسبت به DES معمولی، یک سوم است.
  - نیازمند ۳ کلید است با طول 3 x 56 = 168
- راه حل دیگر: استفاده از دو کلید ولی با دنباله E-D-E:
  - $C = E_{K1}(D_{K2}(E_{K1}(P)))$
  - استفاده از رمزگشایی صرفاً بخاطر سازگاری با پیاده سازی های قبلی DES معمولی بوده است.
    - اگر K1 = K2، متناظر DES معمولی است.
- این روش توسط ANSI و ISO استاندارد شده است.
  - استانداردهای مدیریت کلید ANSI X9.17 و ISO 8732
- تاکنون حمله تحلیل رمزی عملی روی آن شناخته نشده است.
  - هزینه حمله جستجوی جامع آن 2^112 است.
  - هزینه تحلیل دیفرانسیلی آن نیز بیشتر از O(10^52) است.

DES سه تایی



(a) Encryption



(b) Decryption

ساختار رمز فیستل

- ساختار رمز فیستل

اکثر الگوریتم‌های قالبی از جمله DES مبتنی بر روش ارائه شده توسط فیستل Horst Feistel در سال ۱۹۷۳ در IBM هستند.

شبکه فیستل مبتنی بر انتخاب پارامترها و ویژگی‌های زیر است.

۱- اندازه بلوک: هرچه بلوک بزرگتر باشد، امنیت بیشتر است.

۲- اندازه کلید: هرچه کلید بزرگتر باشد، امنیت بیشتر است.

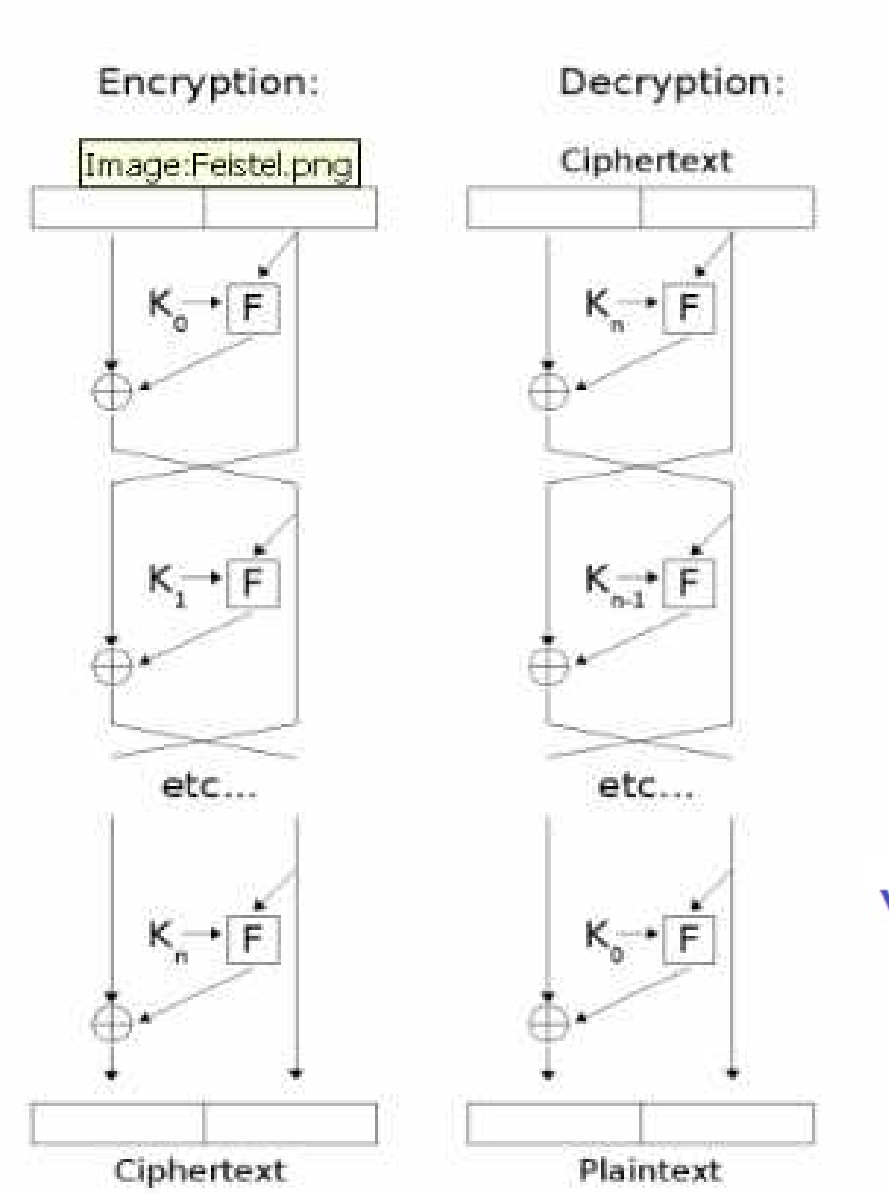
۳- تعداد مراحل: تعداد مراحل بیشتر، امنیت را افزایش می‌دهد.

۴- الگوریتم تولید زیر کلیدها: پیچیدگی بیشتر باعث مشکل شدن آنالیز رمز می‌شود.

۵- تابع هر مرحله: پیچیدگی بیشتر باعث مشکل شدن آنالیز رمز می‌شود.

۶- سرعت نرم‌افزار برای رمزگذاری و رمزگشائی: سرعت در اجرای الگوریتم اهمیت دارد.

۷- سادگی آنالیز



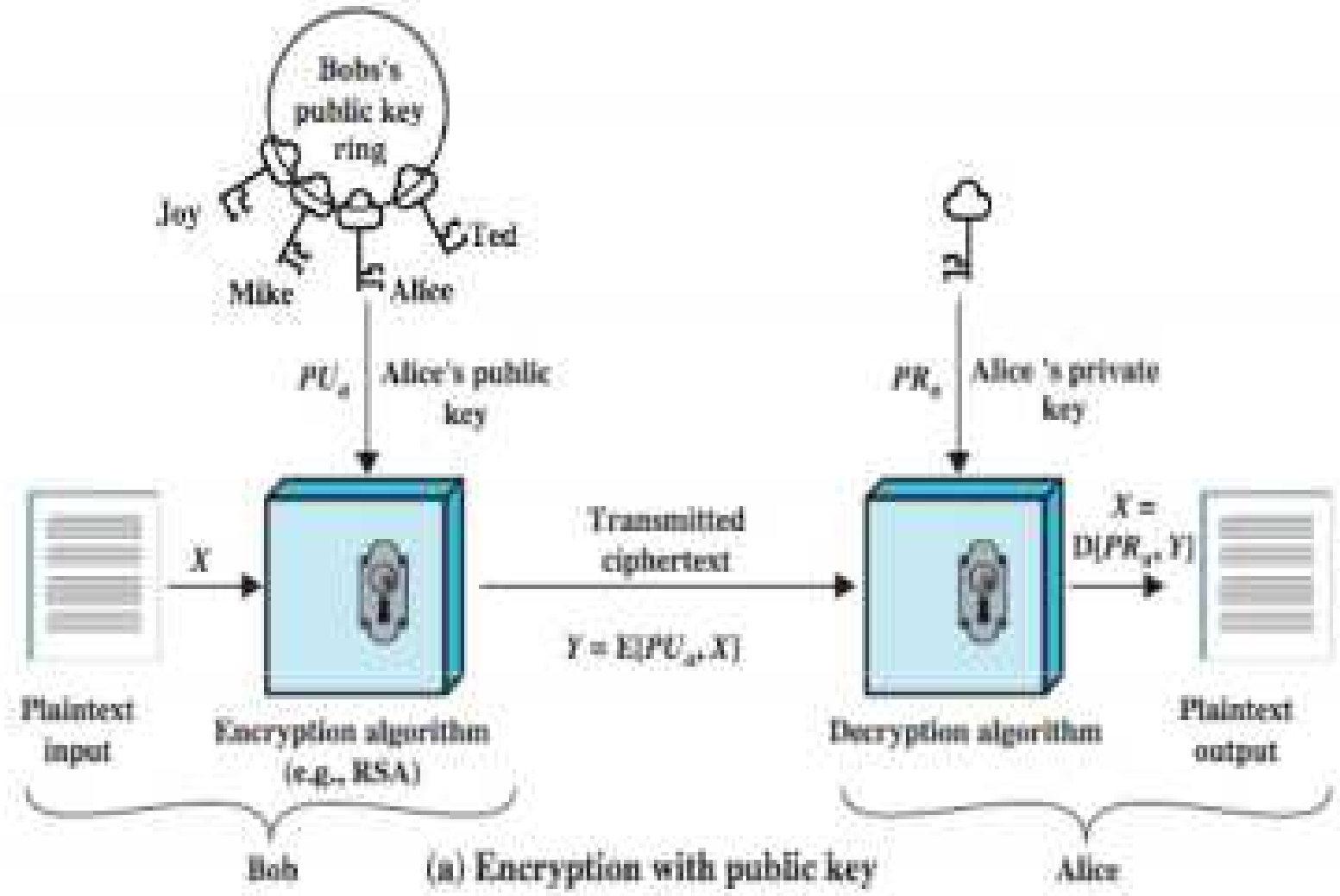
Feistel Cipher

رمزگذاری با کلید عمومی-متقارن

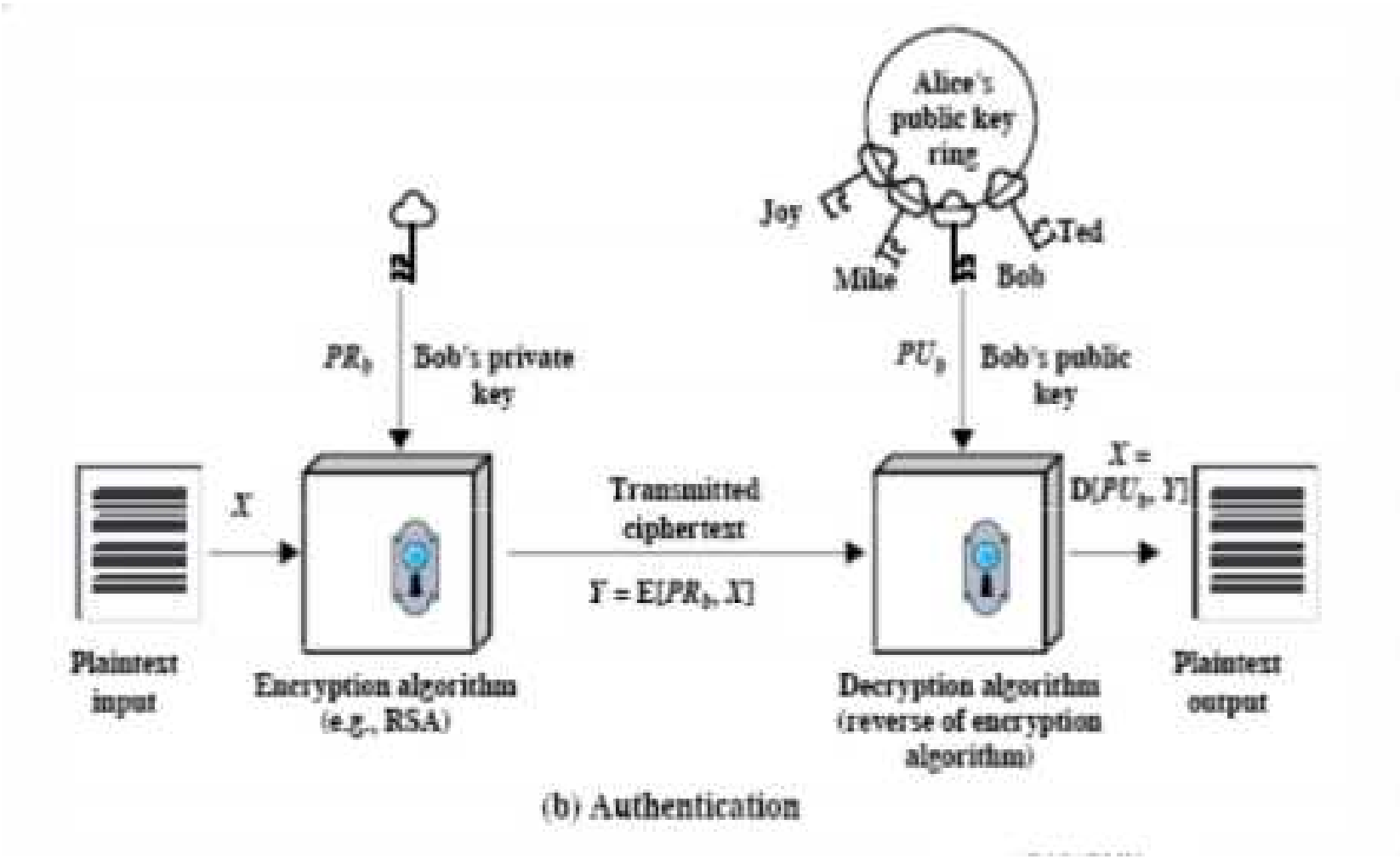
- اصول رمزنگاری با کلید عمومی (Public-Key)
  - استفاده از دو کلید مسائل خود در زمینه‌های زیر را دارد:
    توزیع کلید، محرمانگی و تایید هویت
  - این رمز نگاری ۶ جزء دارد

1. Plaintext
2. Encryption algorithm
3. Public key
4. Private key
5. Ciphertext
6. Decryption algorithm

رمزگذاری با کلید عمومی



رمزگشایی با کلید عمومی



کاربردهای رمزگذاری با کلید عمومی

- کاربردهای رمزنگاری با کلید عمومی
- سه دسته کاربرد دارد

۱- رمزنگاری - رمزگشائی

فرستنده متن مورد نظر را رمز کرده و ارسال می‌کند

۲- امضای دیجیتال

فرستنده پیام را رمز می‌کند

۳- تبادل کلید

دوطرف برای ارسال کلید یک نشست همکاری می‌کنند

مقایسه دو روش متقارن و نامتقارن

مقایسه دو روش متقارن و نامتقارن: روش متقارن یک کلید و در روش نامتقارن دو کلید داریم.

مزیت روش نامتقارن: نیازی به کانال امن جهت کلید نیست و تولید کلید راحت‌تر می‌شود. مشکل تبادل کلید را راحت‌تر می‌کند. کلیدهای با طول بیشتری استفاده می‌شود تا قدرت بیشتری داشته باشد. حجم محاسبات بیشتری لازم است بنابراین از متقارن کندتر است و برای رمزگذاری متن بزرگ مناسب نیست و از روش متقارن استفاده می‌شود. روش متقارن هزینه کمتری دارد.

در روش متقارن توزیع کلید نیاز به کانال امن دارد و دو طرف باید برای کلید توافق کنند و کلید توزیع می‌شود. مثلاً ۵۰۰ نفر باید کلیدها را به صورت امن تبادل کنند. چون راه مناسبی برای این کار وجود ندارد روش نامتقارن پیشرفتی در این زمینه محسوب می‌شود.

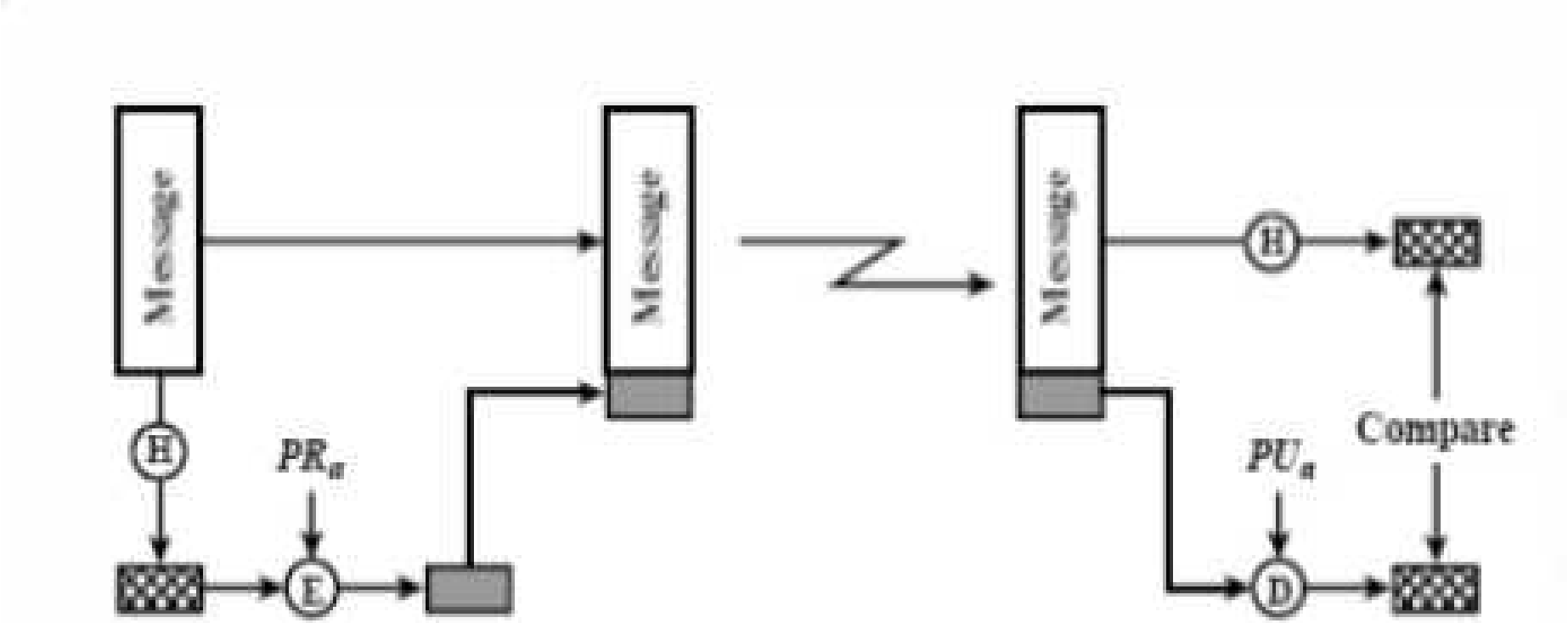
امضای دیجیتال

- یک امضای دیجیتال نوعی رمزنگاری نامتقارن است. هنگامی که پیغامی از کانالی ناامن ارسال می‌شود، یک امضای دیجیتال که به شکل صحیح به انجام رسیده باشد می‌تواند برای شخص گیرنده پیام دلیلی باشد تا ادعای شخص فرستنده را باور کند و یا به عبارت بهتر شخص گیرنده از طریق امضای دیجیتال می‌تواند این اطمینان را حاصل کند که همان شخص فرستنده نامه را امضا کرده است و نامه جعلی نیست

امضای دیجیتال

- امضای دیجیتال در حقیقت همان امضای الکترونیک است و در عوض امضای دستی توسط افراد مورد استفاده قرار می گیرد تا از این طریق هویت فرستنده پیام یا امضا کننده سند ارسال شده مشخص گردد. دولت ایالات متحده آمریکا امضای مزبور را مورد قبول قرار داده و همانند امضاهای دفتری به این نوع امضاء اعتبار و مصونیت بخشیده است.
- قانون مربوط به چک الکترونیک در ژوئن ۲۰۰۰ وضع گردیده است. همچنین تکنولوژی چک الکترونیک امکان آن را فراهم ساخته است تا از امضای دیجیتال برای اسناد خاصی استفاده شود و نه برای تمامی اسناد این مساله باعث می شود بخشی از سند، از قسمت اصلی جدا شده بدون آنکه خدشه ای به انجام امضای دیجیتال وارد سازد. **این تکنولوژی برای قراردادهای تجاری و سایر اسناد قانونی که باید از طریق Web ارسال شوند بسیار مفید می باشد.**

امضای دیجیتال



توصیف امضای دیجیتال

- یک امضای الکترونیکی بر روی سند الکترونیکی مثل یک امضای دست نوشته بر روی سند چاپی می باشد. این امضا مدرکی است که اثبات می کند این شخص آن متن را نوشته است. گیرنده نیز تایید می کند که این پیغام از شخص مورد نظر آمده است و امکان انکار آن توسط فرستنده وجود ندارد.
- امضای الکترونیکی بر مبنای ترکیبی از ایده هش کردن داده به همراه کدگذاری با کلید عمومی می باشد. بیشتر توابع هش مشابه توابع کدگذاری می‌باشد که یک بلاک داده را می گیرند و مکرراً الگوریتم را به منظور تغییر بیتهای آن، بر روی آن اعمال می کنند در نتیجه پیش‌بینی خروجی آن مشکل خواهد بود در نتیجه این عملی نیست که دیتای اصلی را به هر طریقی تغییر دهیم و مطمئن باشیم که خروجی به‌دست آمده با خروجی تابع هش برابر باشد.

گواهینامه دیجیتال

گواهینامه یک سند الکترونیکی است که جهت تعیین هویت یک فرد، یک موسسه، یک سرور و یا یک موجودیت در ارتباط با یک کلید عمومی استفاده می‌شود. همانطور که هرشخص برای اخذ گواهینامه رانندگی نیازمند مراجعه به اداره راهنمایی ورانندگی است و در آنجا از او اطلاعاتی (نام ونام خانوادگی،آدرس و....)جهت تعیین هویت اخذ می شود، CA[1] یا ارائه کنندگان گواهینامه، مسئول احراز هویت موجودیتها و مسایل مربوط به گواهینامه هستند. این ارائه کنندگان می‌توانند افراد ثالث غیر وابسته باشند یا سازمانهایی باشند که خودشان ارائه دهنده گواهی جهت نرم افزارهای سرور باشند. روشهایی که جهت ارزیابی هویت افراد بکار می رود به سیاستهای ارائه دهندگان، موجودیت درخواست کننده و مقصود آنها از این درخواست بستگی دارد. در مجموع یک ارائه کننده باید قبل از انتشاریک گواهی، باید از هویت موجودیتی که درخواست گواهی دارد به درستی مطمئن شود. گواهی که توسط ارائه کنندگان انتشار می یابد یک کلید عمومی را به نام درخواست کننده (مانند نام یک کارمند یا نام یک سرورو...) و امضای دیجیتالی ارائه‌دهنده متصل می کند. این مکانیزم موجب کمک بیشتر به جلوگیری از جعل کلید عمومی به منظور تغییر هویت می گردد زیرا تنها کلید عمومی که گواهی شده است با کلید خصوصی متناظر عمل می کند.

Certificate Authentication

در بحث امنیت ------دیوار آتش:

دیواره آتش سیستمی است که در بین کاربران یک شبکه محلی و شبکه بیرونی مثل اینترنت قرار داردو ضمن نظارت بر دسترسیها در تمام سطوح ورود و خروج اطلاعات را تحت نظر دارد. از سه لایه تشکیل شده است که هر کدام وظایف زیر را بر عهده دارند:

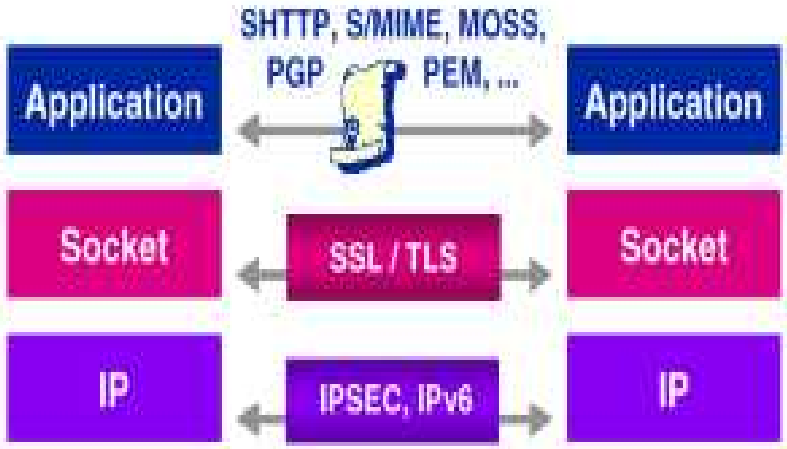
۱. در لایه شبکه دیواره آتش فیلدهای بسته IP را پردازش و تحلیل می کند.
۲. در لایه انتقال دیواره آتش فیلدهای بسته‌های TCP یا UDP را پردازش و تحلیل می کند.
۳. در لایه کاربرد دیواره آتش فیلدهای سرایند و همچنین محتوای خود داده‌ها را بررسی می کند.

توضیحات تکمیلی در رابطه با SSL

Https یک کانال SSL ایجاد می‌کند. قفلی که در پایین دیده می‌شود نشان می‌دهد ارتباط به شکل امن صورت می‌گیرد. با کلیک بر روی آن اطلاعات گواهی دیجیتال مربوط به سایت دیده می‌شود.


Website Identification
USERTrust has identified this site as:
acquirer.samancpay.com
This connection to the server is encrypted.
Should I trust this site?
View certificates
پرداخت الکترونیک سامان
زمان باقیمانده 7:23
اطلاعات کارت
* شماره کارت :
* رمز اینترنتی:
* cvv2:
*تاریخ انقضی کارت :
ماه
سال
* عبارت زیر را وارد نمایید:
تغییر تصویر
پرداخت
بازگشت
نکات امنیتی
اطلاعات پذیرنده
نام پذیرنده : فروش
کد پذیرنده : 7252

ادامه SSL



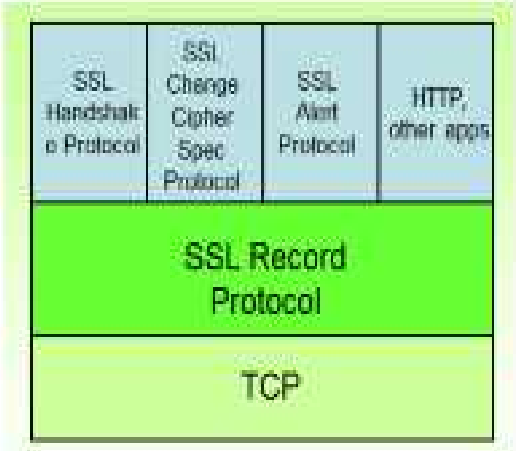
پایین‌ترین لایه لایه‌ی IP است و پروتکل‌های IPSec , IPv6 امنیت را برای این لایه فراهم می‌کند. SSL در لایه سوکت یا Transport است و امنیت را در این لایه فراهم می‌کند. در لایه Application اگر TLS داشته باشید می‌توانید از Https و یا پروتکل‌های دیگر استفاده کنید. سوکت یک کانکشن را ایجاد می‌کند و TLS امنیت این ارتباط را برقرار می‌نماید. TLS پس از اینکه در اینترنت مورد استفاده قرار گرفت نام آن به SSL تغییر یافت.

سرویس هایی که SSLو TLSفراهم می کنند

مهمترین سرویس Confidentiality یا محرمانگی است. اطلاعات را رمز شده ارسال می‌کند. مثلاً اگر جزئیات کارت ارسال می‌شود آن‌ها را رمز شده می‌فرستد. یک کانال امن بین خریدار و فروشنده ایجاد می‌کند. دومین سرویس Authentication یا احراز هویت است. می‌توان طوری تنظیم کرد که هر دو همدیگر را Authenticate کنند. اما مستلزم این است که هر دو گواهی دیجیتال داشته باشند. اما چون اغلب خریداران گواهی دیجیتال ندارند فقط فروشنده Authenticate می‌شود. پروتکل SSL این کار را انجام می‌دهد و فروشنده را Authenticate می‌کند.

کاربردSSL

یکی از رایجترین کاربرد SSL در پرداخت الکترونیک است. مخصوصاً زمانی که پرداخت از طریق کارت انجام می‌شود. در مرورگرهای وب مورد استفاده قرار گرفته است. در IE و Netscape وجود دارد. این لایه دو پروتکل دارد. یکی Record Protocol که در رابطه با Application است و خدماتی را برای این لایه فراهم می‌کند.

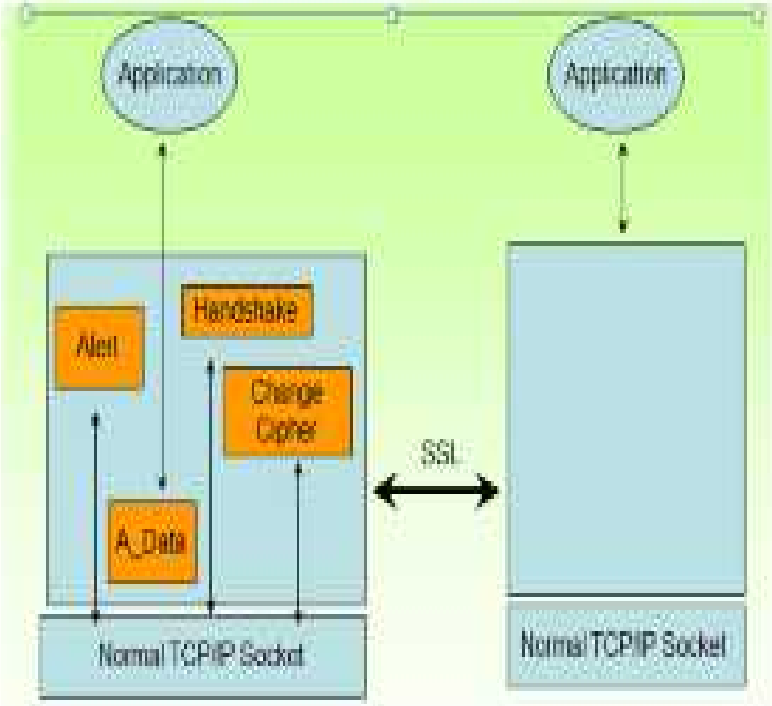


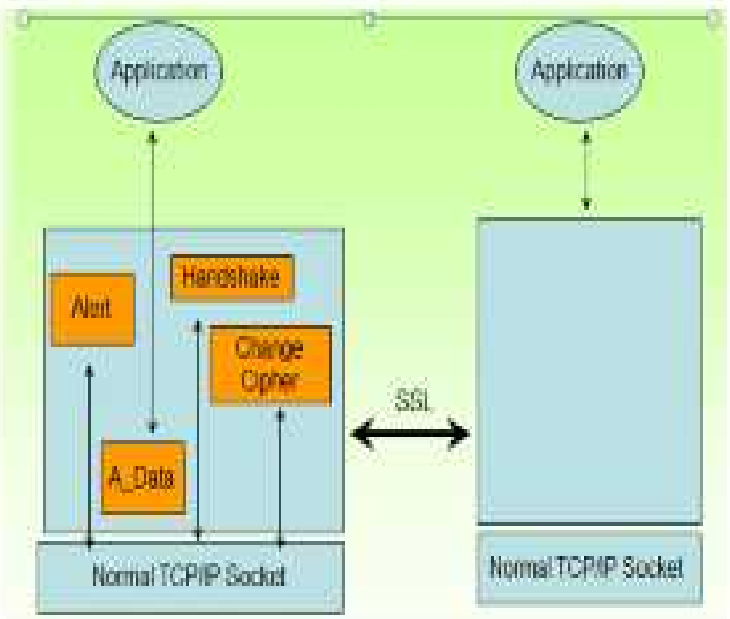
لایه TCP دو لایه به آن اضافه شده است. SSL Record Protocol و Hand Shake Protocol، SSL Change Cipher Spec Protocol، SSL Alert Protocol و HTTP and Other apps.

پروتکل‌های شبکه از چند لایه تشکیل شده است. در TCP/IP یک لایه Transport است. خدماتی برای لایه بالاتر ارائه می‌کند. قابلیت-های امنیتی در TCP در نظر گرفته نشده است. برای اینکه امنیت برقرار کنیم باید از SSL اضافه کنیم.

اجزای پروتکل SSL

اجزای پروتکل SSL: اگر SSL نداشته باشیم Application مستقیم با TCP در ارتباط است. اما اگر SSL داشته باشیم اطلاعات به صورت رمز شده ارسال می‌شود.





A_Data پروتکلی است که پیغام را رمز می‌کند. پروتکل Hand Shake بر روی الگوریتم رمزنگاری و کلید مورد استفاده توافق کنند. اگر نیاز به احراز هویت هست نیز صورت گیرد. در ابتدای برقراری ارتباط صورت می‌گیرد. از هویت سرویس دهنده اطمینان حاصل می‌شود. Change Cipher اگر نیاز به تغییر پارامترهای رمزنگاری باشد انجام می‌دهد. اگر مشکلی در ارتباط SSL ایجاد شود پروتکل Alert هشدار مناسب را فراهم می‌کند.

پرداخت الکترونیک با استفاده از SSL: فقط سمت سرویس دهنده احراز هویت می‌شود. تمام ارتباط‌ها باید رمزنگاری شود.

چک الکترونیکی

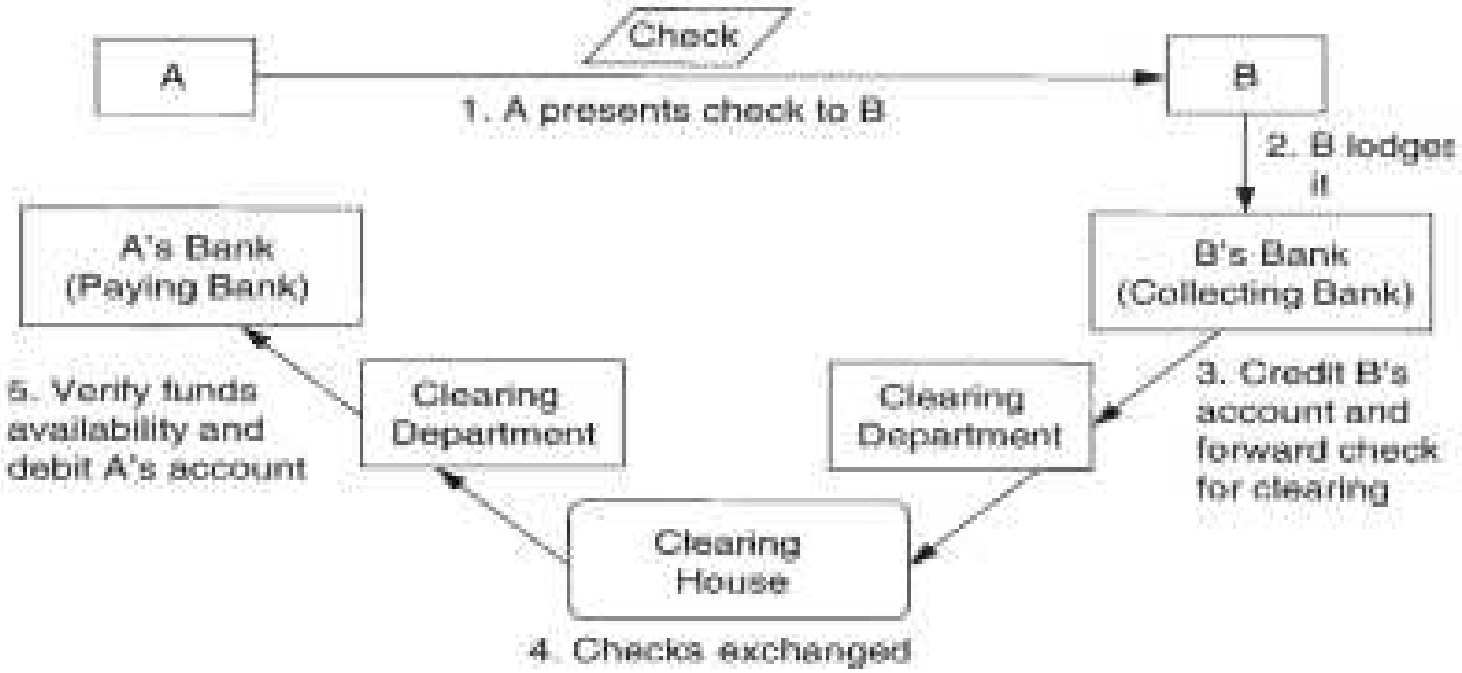
چک‌های الکترونیکی

استفاده از چک‌های کاغذی در حال کاهش است، به جای آن از روش الکترونیکی برای دستور پرداخت استفاده می‌شود. با از Debit Card استفاده می‌شود. قبلاً هم گفته شده که چک الکترونیکی همانند Debit Card است.

دو نوع پرداخت داریم: پرداخت مستقیم و غیر مستقیم. پرداخت مستقیم به گیرنده وجه توسط خود شما انجام می‌شود. در غیر مستقیم دستوری صادر می‌کنید که از حساب شما کم شود و به حساب طرف مقابل واریز نماید، همانند چک.

ادامه چک الکترونیکی

چک: یک دستور پرداخت است. از حساب فرد کم شده و به حساب فردی که اسم وی روی چک است ارسال می‌شود.



ادامه چک الکترونیکی –توضیح مربوط به شکل اسلاید قبل

اگر گیرنده و صادرکننده چک در یک بانک باشد از حساب صادر کننده کم و به حساب گیرنده واریز می‌شود اما اگر حساب در بانک‌های مختلف باشد چک به صورت تصویر فوق پاس می‌شود. چکی که A صادر کرده تحویل فرد B می‌شود. گیرنده در مرحله دوم چک را به حساب خود در بانک خود می‌خواباند. مرحله سوم حساب B شارژ می‌شود و این مبلغ به حساب وی واریز می‌شود. (این اتفاق در ایران نمی‌افتد اما در برخی کشورها همانند کانادا چک درون دستگاه خودپرداز وارد کرده و همان لحظه این مبلغ به حساب واریز می‌شد). سپس چک برای Clear شدن Forward به Clearing House ارسال می‌شود. Clearing House اتاق پایاپای است و هر بانکی برای خودش بخش Clear دارد. این چک‌ها به این بخش ارسال می‌شود. نهایتاً چک مربوط به بانک A به آن بانک ارسال می‌شود. سپس چک می‌شود حساب A موجودی دارد. اگر داشت از حساب کم می‌شود. (در ایران پس از پاس شدن چک، چک در بانک B به حساب فرد B واریز می‌کند).

سیستم های متمرکز

سیستم‌های متمرکز: سیستم‌های مالی آنلاین که به صورت متمرکز فعالیت می‌کنند. مبلغی را به صورت آنلاین از حسابی کم و به حساب دیگری اضافه می‌کنند نیازی به شبکه دیگر برای Clearing ندارند. همانند سیستم‌های Paypal. حساب مشتریان در یک سیستم قرار دارد و از یک حساب کم و به حساب دیگر پرداخت می‌شود. برای زمانی که افراد در بانک‌های مختلف حساب داشتند عمل Clearing نیاز داریم. وقتی سیستم متمرکز باشد دیگر نیازی به عملیات Clearing نیست.

مثال:

BidPay	www.bidpay.com
Billpoint	www.billpoint.com
C2it (Citibank)	www.c2it.com
CheckSpace	www.checkspace.com
Cybergold	www.cybergold.com
Ecount	www.ecount.com
E-gold	www.e-gold.com
eMoneyMail	www.emoneymail.com

سایر نمونه سیستم های متمرکز

Billpoint Payment System مربوط به سایت eBay بود این سیستم ایجاد شده تا کالاهایی که در حراجی آنلاین خرید شده پرداخت صورت گیرد.

Internet Cash یک حساب متمرکز ایجاد شده که پرداخت به فروشندگان آنلاین صورت گیرد.

Rocket Cash: بخشی برای کنترل والدین نیز اضافه کرده است.

Pay Palیک ابزار مطمئن برای نقل و انتقال پول است.

- **Pay Palیک ابزار مطمئن برای نقل و انتقال پول است**
- **PayPalیک سرویس واسط برای خریدهای آنلاین است. این سرویس آنچنان دارای اعتبار و اعتماد شده است که بالغ بر ۹۵ درصد خریداران eBayاز آن بهره می‌برند.**
- این کمپانی در کشور آمریکا قرار دارد و بیش از یکصد میلیون کاربر در سطح جهان از این حساب برای خرید ، فروش و کلیه پرداخت های خود استفاده می کنند و بعلت امنیت و هماهنگی با کلیه کارت های اعتباری و حساب های بانکی محبوبیت بسیار زیادی در بین کاربران اینترنت دارد.

Paypal یک سایت تجارت الکترونیک که کاربران مستقل از حساب بانکی و کارت اعتباری یک حساب در آن ایجاد می‌کنند. Paypal حساب کاربران خود را نگهداری می‌کند. Paypal مانند هر فروشگاه الکترونیکی از یک بانک خدمات می‌گیرد تا مشتریان پرداخت را از طریق آن درگاه انجام دهند. عملاً هر پرداخت به حساب اصلی Paypal انجام می‌شود و اعتباری که در حساب Paypal است می‌توانید پرداخت را برای دیگران انجام دهید.

paypal

وقتی حسابی همانند Paypal باز می‌کنید چگونه مبلغ به این حساب واریز می‌شود؟ چه راه‌هایی برای انتقال حساب وجود دارد؟ دو روش رایج وجود دارد. انتقال از طریق کارت اعتباری و یا از طریق حساب جاری که در بانک فیزیکی وجود دارد مبلغی را به حساب Paypal واریز کنیم.

وقتی حسابی را می‌خواهید باز کنید ابتدا باید از طریق SSL به Paypal وصل شوید و سپس اطلاعاتی را Paypal درخواست می‌کند.

- name,
- address,
- contact details of the account owner
- physical bank account details

سپس از حساب جاری یا کارت اعتباری به حساب Paypal لینک شده و مبلغ تعیین شده از حساب کم و به Paypal واریز می‌شود.

روش برداشت و مدل درآمدpaypal

برداشت از حساب Paypal: ممکن است بخواهید از حساب Paypal برداشت کنید. در برخی سیستم ممکن است این امکان وجود نداشته باشد. اگر شماره حسابی معرفی کرده باشید Paypal می‌تواند این مبالغ را به آن حساب منتقل نماید. سیستم‌های قدیمی‌تر چک رو صادر می‌کرد و با پست ارسال می‌کردند.

مدل کسب و کار حساب متمرکز: مهمترین منبع درآمدی این حساب‌ها از روی سود منابع در Paypal و کارمزد مربوط به تراکنش (Transaction Fee) و تبلیغات می‌باشد.