سیستمهای پرداخت الکترونیک

پرداخت چیست؟

نقل و انتقال وجه (نقدی/غیرنقدی) از حسابی به حساب دیگر بابت هزینه های انجام شده (سرویس/کالا)که میتواند بصورت دستی یا الکترونیکی باشد.

بازیگران این صنعت

خریدار (سرویس گیرنده)

X (رابطه)

فروشنده(سرویس دهنده)

بانک
اسکناس
سخت افزار/امنیت
نرم افزار App.
شرکتهای واسط (PSP)

Online
ATM
POS

24/7
۷ روز هفته/۲۴ ساعت
For (Everybody,Everytime,Anywhere)

Profitibility
نمودار سوددهی/سختی کار

C	D
A	B

Difficulty

A (سود دهی کم–سختی کار کم) کارت به کارت کردن

B (سود دهی کم–سختی کارزیاد) خرید شارژ

C (سود دهی زیاد–سختی کار کم) خرید online ،پرداخت

D (سود دهی زیاد–سختی کارزیاد) کارت هوشمند سوخت

مورد D مورد توجه است ،چون پایدارتر می باشد ،امکان ورود همه رقبا کم است و بعد از موفقیت در تجارت جلوتر از رقبا خواهیم بود.

مورد A دارای بیشترین بازار رقابت میباشد.

اطلاعات مورد نیاز برای پرداخت الکترونیکی

۱–کد:شماره کارت ۳– CVV2 :رمز دوم کارت

۲–رمز عبور ۴–تاریخ انقضاء

ویژه گیهای پرداخت الکترونیکی بر اساس نیاز کاربران از منظر موضوعی

ویژه گی	با تمرکز بر نیاز
امنیت	مشتری،فروشنده ،صادرکننده
اعتبار	مشتری،فروشنده ،صادرکننده
بی نامی/گمنامی	مشتری
تمرکز زدائی (از یک دستگاه به بانک)	مشتری،فروشنده ،صادرکننده
مقبولیت	مشتری،فروشنده ،صادرکننده،پذیرنده
کارائی	مشتری،فروشنده ،صادرکننده
مشتری گرایی	فروشنده ،صادرکننده
انسجام	صادرکننده
سهولت	مشتری
انعطاف پذیری	مشتری،فروشنده
هزینه پایین	مشتری،فروشنده

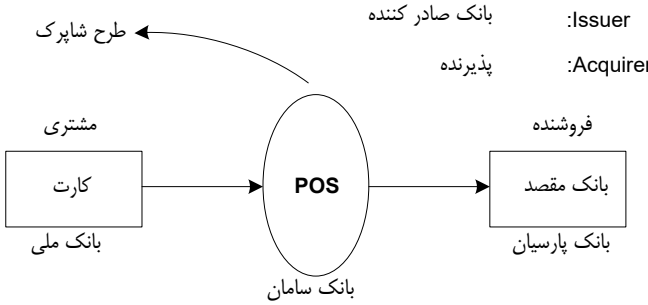
معرفی چهار Role

Payer: پرداخت کننده(مشتری)–مبداء حساب(کارت) صاحب کارت

Payee: دریافت کننده (بانک ،کارگزار یا صاحب مقصد)–فروشنده

Issuer: بانک صادر کننده

Acquirer: پذیرنده



Payer: ملی،ملی
Payee: پارسیان،سامان
Issuer: ملی،ملی
Acquirer: شرکت سرویس دهنده سامان، شرکت سرویس دهنده سامان

انواع پول سنتی

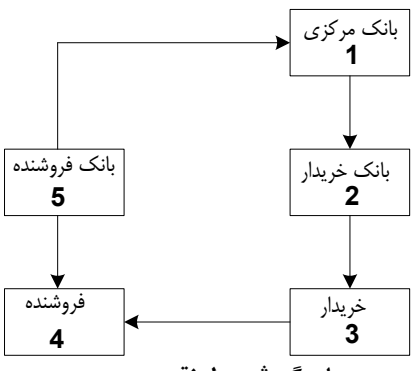
رسمی (Fiduciary) مرجع خرید و فروش در هر جامعه(بصورت کاغذی بوده و توسط بانک مرکزی منتشر میشود)

غیر رسمی (Scriptural) چک پول بانکها وحسابهای بانکی و... که توسط سایر بانکها (غیر از بانک مرکزی) انتشار میابد.

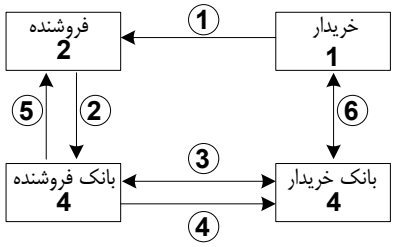
فیزیکی (Token) هر پول رسمی و غیر رسمی که قابل لمس باشد.

مستند (National) هر پول رسمی و غیر رسمی که غیرفیزیکی باشد.(در حسابهای شخصی و حقوقی نزد بانکها موجود هستند) (اوراق بهادار)

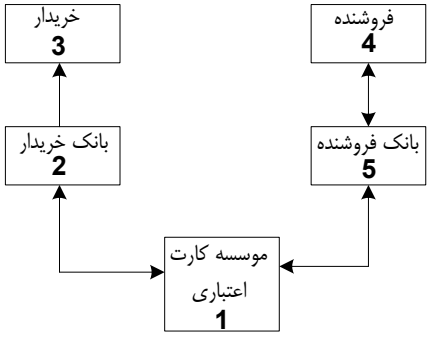
هایبرید (Hybrid) پولهایی که بصورت بالقوه پول رسمی یا غیر رسمی را تشکیل میدهند و جهت نقد کردن آنها باید یک اقدام دیگری در مورد آنها صورت پذیرد.مانند چکها و کارتهای اعتباری



جریان گردش پول نقد



جریان گردش چک



جریان گردش پول بصورت کارت اعتباری

حداقل ویژه گیهای مورد نیاز برای ایفای نقش پول (واسطه) در مبادلات اقتصادی و تجاری

-پذیرش جهانی (مخصوصا برای پولهای الکترونیکی
-قابلیت انتقال و حمل ساده
-گمنامی یا نا مشخص بودن صاحب آن و یا پرداخت کننده آن
-ازایمنی مناسب برخوردار باشد (فراموش نشود ،براحتی سرقت نشود،.....
-شخصی بودن (فقط صاحب آن از مقدار آن مطلع باشد)
-قابلیت استفاده بصورت روی خطی و غیر رو خطی (Offline)
-قابلیت تبدیل به پول خرد

هزینه پول

پول اعم از نشر و توزیع و حفظ و نگهداری آن دارای هزینه است. و ابعاد آن عبارتند از :

-زمان یا مدت زمانی که برای فرایند آن بایستی صرف شود (اعن از نشر و توزیع و حفظ و نگهداری و مصرف آن)
-میزان ریسک نهفته در فرایند فوق
-هزینه های فیزیکی فرایند فوق (هزینه نقل و انتقال پول ،هزینه های ایمنی ،هزینه های قانونی و اعمال قانون در مواقع سوء استفاده ،...)

انواع ریسک در پرداخت پول

ریسکهای اجرایی سیستم

ایمنی از جهت دسترسی افراد مجاز ،سو استفاده کارکنان ،جعل پول الکترونیکی ،طراحی سیستم ،اجراو نگهداری آن ،استفاده های نادرست مشتریان ،ریسک مربوط به ارائه کننده خدمات و سیستم مالی ،دوره عمر سیستم ،دوبارگی نقل و تنتقال پول توسط مشتری پس از دریافت آن در مرحله اول Repudiation

ریسکهای اعتباری سیستم Reputation

وجود افکار عمومی منفی که منجر به شکست میشود ،کاستی های سیستمی ،پاسخگو نبودن سیستم در برابر مسئولیتها و...

ریسکهای قانونی

عدم تعهد و رعایت قوانین ،پول شوئی ،عدم رعایت اطلاعات شخصی ،در نظر نگرفتن قوانین کشورهای دیگر در هنگام انجام معاملات بین المللی و....

ریسکهای بانکی

نرخ بهره ،تحولات بازار پولی،شرایط اقتصادی و سیاسی و...

ریسکهای جرمی

سو استفاده ها ،تقلب ها ،دزدی ،سرقت و.....

فرآیند پرداخت الکترونیکی
American Express

Authentication	Authorization	Value Exchange	Financing	Accounts Receivable Mgmt.	Information Reconciliation Reporting	Dispute Ressolution Servicing
احراز هویت	تایید هویت	نقل و انتقال	تایید مالی	فاکتور	گزارش تراکنشی	خدمات پس از فروش
درخواست	تایید ورود	Transfer		Factor	برای بانک مقصد	Customer
Verify	Allow					

۱: شناسایی مصرف کننده و فروشنده ۲: تایید صحت نقل و انتقال ۳:ایجاد اعتبار لازم ۴:ایجاد مستندات الکترونیک و حل مشکلات و اختلاف نظرها

E-Payment Services			
-Electronic Bill presentment	-International Payments	-Trade Receivable Account	-installment Loans(specific to transaction)
-Line of credit (for use across multiple sites)		-lease (specific to transaction)	-charge card products

مزایای پرداخت الکترونیک

-کاهش هزینه ها
-تسریع فرایند
-حذف کاغذ بازی و بوروکراسی
-امکان پرداخت و دریافت در سطح جهانی

یک پرداخت کی به اتمام میرسد؟

ابزارهای خرید اتوماتیک
Purchasing Automation Tools

میزان خرید بر حسب پول رایج

Staples: نوشت افزار (مامور خرید)
Speciality: انرژی (سوخت)
Strategic: قیمت تمام شده
Biz Retail: خرید روزانه (مغازه دار) ،متنوع

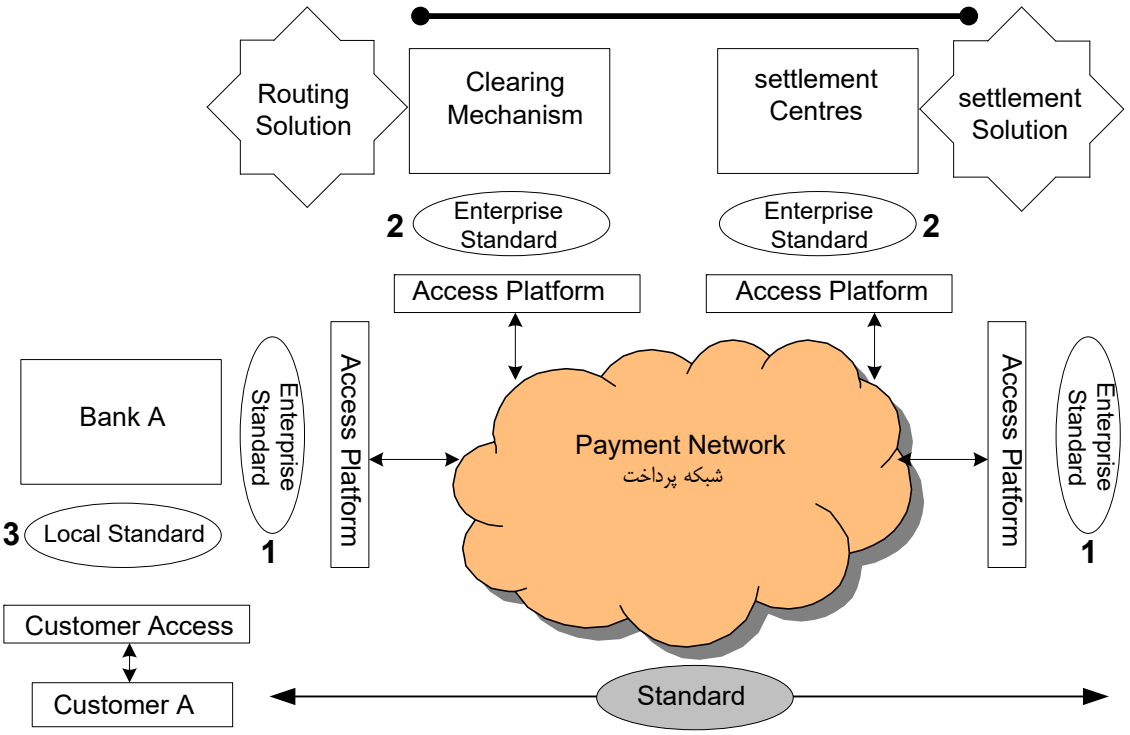
Speciality کالای خاص ERP,EDI	**Strategic** استراتژیک ERP,EDI
Biz Retail خرید جزعی Pretty cash card T&E Cards	**Staples** خرید عمده E-purchasing E-Commerce

High ↑ Low
دوره تناوب خرید High →

مدلهای سیستم پرداخت
Perchasing Automation Tools

	Limitations محدودیتها	Benefits مزیتها/سود	Level of data details وضعیت جزئیات داده ها
EDI Client/supplier (**E**lectronic **D**ata **I**nterchange)	High cost هزینه بالا Complex Supplier enablement(non scalable) پیچیدگی تهیه ابزار و ادوات Lake of consolidated billing فاقد صورتحساب یکپارچه	Client/supplier data interchange تبادل اطلاعات بین client/server Transaction Tracking پیگیری تراکنش	High Direct Cost(COGS) تعدد
ERP (**E**nterprise **R**esource **P**lanning)	High end user implementation cost هزینه راه اندازی و نگهداری بالا Complex Enterprise implementation Usability Barriers نوع کاربری قابل تغییر نیست Inflexible-strict rules cumbersume قوانین غیر منعطف سخت	Automated requisition process تبادل اطلاعات بصورت آنی انجام میشود Transaction tracking قدرت پیگیری درخواست وجود دارد Central data داده متمرکز	
E-Perchasing (Internet Buying)	Lake of robust reporting tools فاقد ابزار قوی گزارش گیری High cost هزینه بالا Complex Supplier enablement پیچیدگی تهیه ابزار و ادوات Lake of reconciliation tools تلفیق ابزار سخت است	Client/supplier data interchange تبادل اطلاعات بین client/server Transaction tracking قدرت پیگیری درخواست وجود دارد Automated work/flow approval report چرخش اطلاعات اتوماتیک	Indirect OPEX Commodities کالا(مواد اولیه ،مصرفی)
Commodity (Perchasing Card) کارت خرید کالا پول غیررسمی	Lake of approval routing for large expense dollar item محدودیت حوزه خرید Lake of sourcing tools for end-users محدودیت تنوع خرید (تاریخ و مبلغ) برای استفاده کنندگان	Low implementation Cost راه اندازی کم هزینه Consolidated invoicing ادغام صورتحساب Robust payment,reporting and reconciliation tools تلفیق قوی ابزارهای پرداخت و گزارشگیری	
Petty Cash (Perchasing Card) بن کارت مانند تنخواه	Limited data محدودیت دیتا (مبلغ) Non -strategic استراتژی و ردیابی خاصی ندارد Lack of preferred supplier utilization فاقد کاربردهای عمومی	End-user convenience tool خیلی در دسترس است. Alternative to petty cash قابل استفاده برای هر کاربری	Low Indirect OPEX petty cash خرد

پرداخت الکترونیکی در سطح بین المللی
Common Infrastructural Elements



برای بهره گیری از بهترین ارتباط پردازشی مستقیم (Straight-Through-Processing :STP) مجموعه عوامل ذکر شده بالاباید با رابطهای کاربری اتوماتیک (Automated –Interface) مجهز گردیده و ارتباط بین بانکی مشتریان نیز بخوبی برقرار باشد.

Local Standard استاندارد تعریف شده ارتباطی محلی که در این حالت استانداردها میتواند متفاوت باشد.

Enterprise Standard استاندارد تعریف شده ارتباطی اختصاصی (دو طرف ارتباط استاندارد یکسان دارند)

Customer مشتری

Customer Access ابزار مشتری برای دسترسی به بانک

Standard استاندارد تعریف شده ارتباطی

Access Platform استاندارد تعریف شده ارتباطی بین بانکی

Clearing Mechanism مرکز تسویه

1 بالاترین سطح استاندارد

2

3 پایینتر از سطح استاندارد ۱

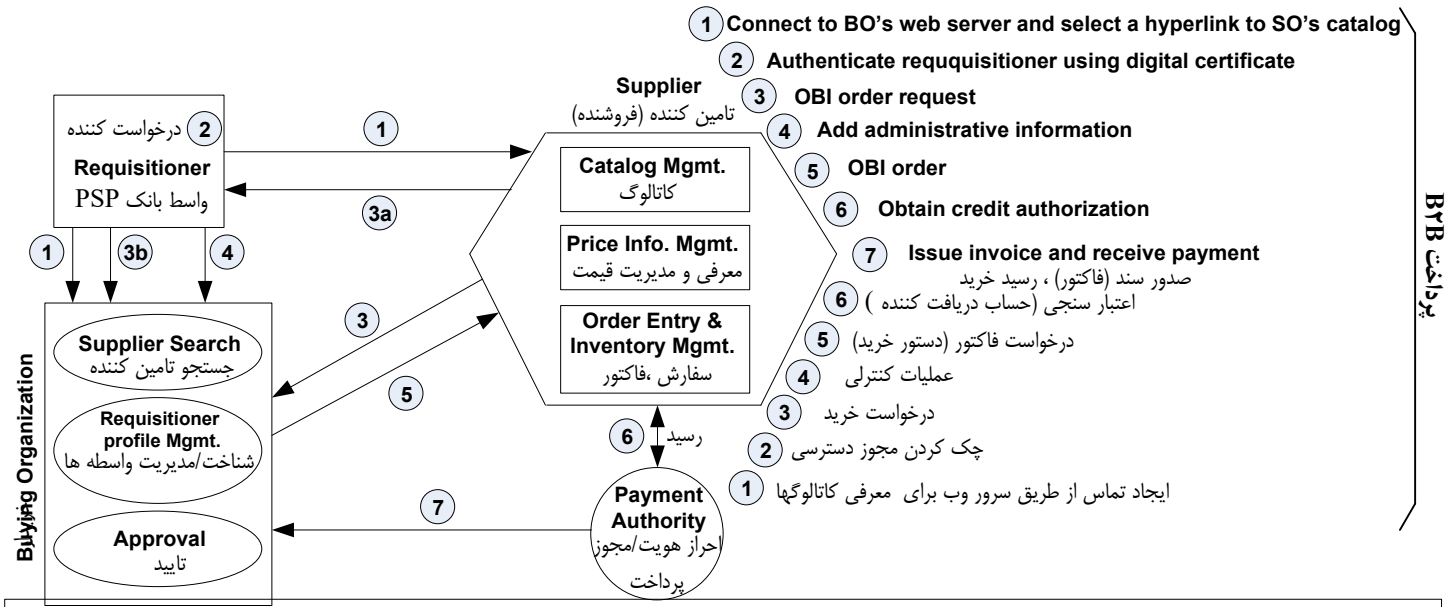
Settlement Solution راه کارهای مدون و اختصاصی

Settlement Centres اتاق فکر (مرکزی)

Routing Solution مواردی مانند مغایرت گیری

واسطه ها چه کار میکنند؟

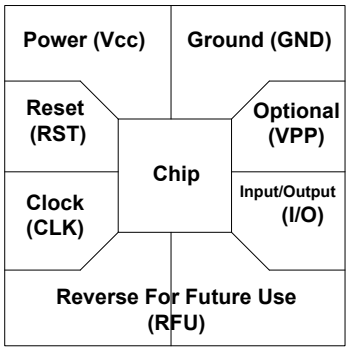
پرداخت B2B
B2B Payment



Electronic Payment
انواع پرداخت الکترونیکی

- Non-internet E-payment — پرداخت غیر اینترنتی — SWIFT,CD network,Giro EDI,Credit Card network
- Internet E-payment — پرداخت اینترنتی — E-Cash (پول الکترونیکی) — Credit Card (CC) (کارتهای اعتباری)
- Others(Mobile,ARS) — پرداخت با موبایل — E-Cheque (چک الکترونیکی) — Micro Payment (پرداخت جزعی)

(SC)
Smart Cards
کارت هوشمند



–ظاهر این کارت شبیه کارت اعتباری میباشد.
–مانند کارت بنزین –کارت تلفن –پول الکترونیکی
–در ارتباط با سوء استفاده های احتمالی هوشمند میباشد.

انواع کارت هوشمند

- **حافظه کم ۱۴۰بایت:** **Magnetic Strip** هزینه برابر کارتهای اعتباری CC
- **با حافظه ۱ الی ۴ کیلوبایت:** **Vanilla memory card** (no processor) ۱ الی ۲.۵ دلار
- **با حافظه ۴ مگابایت:** **Optical memory card** ۷ الی ۱۲ دلار
- **دارای میکرو پروسسور:** **Microprocessor card** ۸ الی ۱۶ کیلو بایت ROM و ۵۱۲ بایت RAM ۷ الی ۱۵ دلار
  –مدل میکروپرسسور ۳۲بیتی به بازار آمده است.

– مزایایی که کارتهای هوشمند نسبت به نقاط منفی پول نقد دارند عبارتند از: چاپ و نشر و تعویض آن ،جعل آن ،حمل آن ،ایمنی آن ،عدم خوانایی آن و.....[پول کاغذی] میباشد.

–ساختار تشکیل دهنده یک کارت هوشمند عمدتا در چیپس یا IC آن که نوعی میکروپرسسور میباشد نهفته است.

–اطلاعات یا محتویات اطلاعاتی هر کارت بر خلاف چته کوچک آن بسیار متعدد بوده و و یژه گی چند کاره بودن کارت هوشمند را بوجود می آورد.

– ساختار نرم افزاری کارت هوشمند شامل دو بخش میشود. ۱–ساختار فایل ۲–مدیریت پایگاه داده در کارت

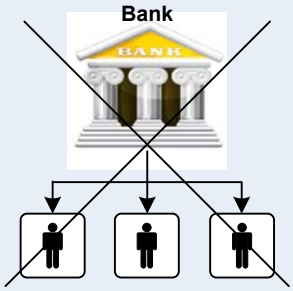
مزایا و معایب کارتهای هوشمند

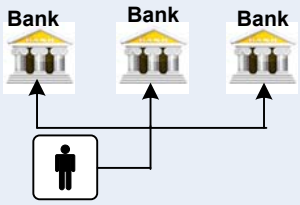
مزایا:
–مناسب برای انواع پرداختهای خرد و تا حدودی متوسط
–قابلیت ناشناختگی منبع پرداخت
–امکان ذخیره سازی پول الکترونیکی در حافظه آن
–ایمنی بالا

معایب:
–برای فعالیتهای تجاری B2B و تا حدودی B2C مناسب نمیباشد.
–هزینه زیر ساختار آن بالا است و برای C2C مناسب نمیباشد.
–هنوز کاربری گسترده پیدا نکرده است.
–در صورت صدمه دیدن یا مفقود شدن کارت براحتی مشکل ساز میشود.

ضرورت سیستمهای غیر بانکی در پرداخت الکترونیکی

-با تغییرات مستمر در شرایط جهانی از جمله با حضور شبکه اینترنت
ضرورت بوجود آمدن سیستمهای جانبی و مکمل تر بوجود آمده است.
-با تغییرات ایجاد شده،مشتری محوری که بر اساس دسترسی
هرچه بهتر به پول استوار شده،در حال حاکم شدن است.





سرویسهای پرداخت الکترونیکی
E-Payment Services

Electronic Bill Presentment صورتحسابهای الکترونیکی (مانند قبض تلفن همراه،صورت مالی ۶ ماهه)
International Payments پرداختهای بین المللی
Trade Receivable Account وصول از دیگران(دریافت وجه=وصول)
Installment Loans (specific to transaction) وام های راه اندازی کسب و کار (سرمایه در گردش)
Line Of credit (for use across multiple site) LC خط ارتباط
Lease (specific to transaction) خطوط ارتباطی اجاره ای (اختصاصی برای کارهای خاص)
خرید از طریق کارتهای قابل شارژ (مانند کارت سوخت)

نحوه عملکرد انتقال الکترونیکی وجوه بطور ساده و بدون در نظر گرفتن امنیت

روشهای انتقال وجه

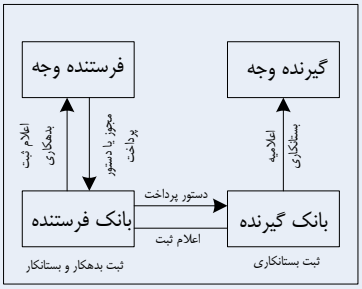
انتقال اعتبار

-وجوه از طریق انتقال دهنده به انتقال گیرنده ارسال میشود.

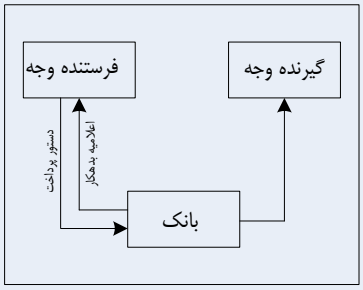
-اگر هر دو دارای حساب بانکی باشند،انتقال دهنده به بانک دستور میدهد حساب خود را بده کار و حساب گیرنده رادر بانک یا بانکهای دیگر بستانکار نماید.

-اگر انتقال دهنده دارای حساب بانکی نباشد.پول را نقدا به بانک پرداخت مینماید و از بانک میخواهد تا حساب انتقال گیرنده را بستانکار نماید.

-اگر انتقال گیرنده دارای حساب بانکی نباشد ،بانک انتقال دهنده متعهد میشود تا پول را بصورت نقد در اختیار انتقال گیرنده قرار دهد.



فرایند انتقال وجه با وجود دو بانک



فرایند انتقال وجه با وجود یک بانک

انتقال بدهکار

-به آن جمع آوری مطالبات نیز میگویند و عبارت است از اخذ اعتبار بوسیله گیرنده از انتقال دهنده تا مبلغ خاصی را از انتقال دهنده از طریق بانک گیرنده وصول نماید.

سه عنصر اصلی انتقال وجه

مجوز پرداخت

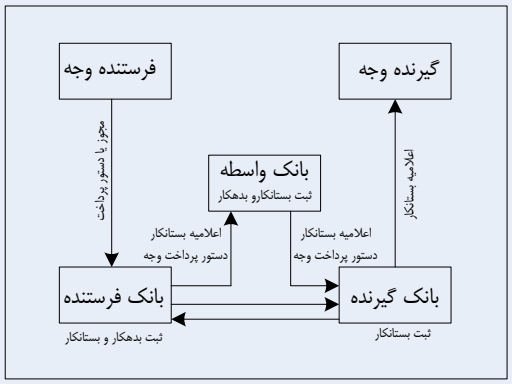
-فرستنده وجه باید مجوز پرداخت را صادر نماید و به بانک اطلاع دهد تا انتقال وجه صورت پذیرد. از طریق (فاکس ،تلکس،کامپیوتر،تلفن همراه ،کارتهای بانکی ،.....)

تهاتر پرداخت

-بانک فرستنده وجه و بانک گیرنده وجه به یک روش توافق برای انجام مبادله پرداخت نیاز دارند که به آن تسویه پرداخت میگویند.

تسویه پرداخت

-بانک فرستنده و گیرنده باید از یک روش پذیرفته و مجاز برای تسویه حساب استفاده کنند.ممکن است هرکدام از بانکها یک حساب در بانک متقابل و یا بانک مرکزی داشته باشند.



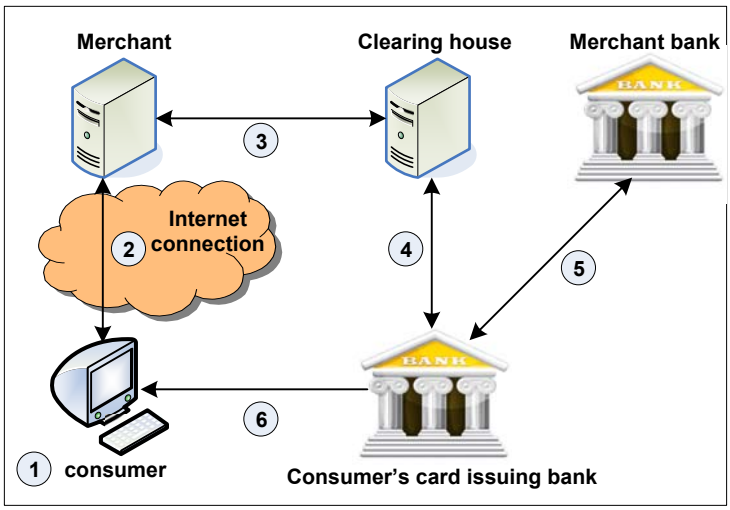
فرایند انتقال وجه با درگیری همزمان سه بانک

پرتکل SET
Secure Electronic Transaction

با توجه به مشکلاتی که روش پرداخت الکترونیک به کمک کارت اعتباری ایجاد نموده بود ،مخصوصا از نظر ایمنی نقل و انتقالات مالی ،شرکتهای (Visa & Mastercard) به کمک هم پرتکل Secure Electronic Transaction (SET) را تدوین نمودند که به کمک آن امنیت نقل و انتقال مالی در اینترنت از طریق بکارگیری یک تاییدیه دیجیتالی Digital Certificate هویت فرستنده را مورد شناسایی و تایید قرار میداد.

مراحل پرداخت الکترونیکی با کارت اعتباری و استفاده از پرتکل SET
Electronic payment [credit card (CC)]

مراحل پرداخت الکترونیکی با کارت اعتباری
Electronic payment [credit card (CC)]



SET:Secure electronic Transaction تبادل الکترونیکی ایمن

1. Consumer mekes purchase 9select "payment with SET" option)
مصرف کننده درخواست خرید کالایا سرویس را میدهد.
2. Merchant and consumer computers verify each other's identify.SET encrypted and Authenticated order and payment information sent to merchant server with SSL.
بانک پذیرنده از یک بستر امن این درخواست را دریافت میکند (SSL)
3. Merchant software contacts clearing house and forwards encrypted message with secure line
درخواست دریافت شده از طریق نرم افزار توسط یک خط مطمئن به بخش تسویه ارسال میگردد
4. Clearing hpuse verifies account and balance with issuing bank
استعلام موجودی و ماهیت دارنده از بانک صادر کننده
5. Issuing bank credits merchant account and transfers funds to merchant bank
ایجاد اعتبار توسط بانک صادر کننده به بانک پذیرنده
6. Monthly statement issued with debit for purchase

-خرید با کارت اعتباری گرانترین روش پرداخت بوده بنابراین برای خریدهای کوچک و بزرگ مناسب نیست و مزیت آن فراهم کردن خرید اعتباری در تجارت الکترونیک میباشد.

-در حال حاضر این روش توسط شرکتهای cyber source,cybercash,verifone در اینترنت ارائه میشود.هزینه اولیه آنها حدود پانصد دلار و هزینه ماهیانه آن حدود۲۰ دلار و برای هر نقل و انتقال حدود ۲۰سنت میباشد.

-شرکتهای visa,mastercard جهت امنیت نقل و انتقال الکترونیکی پرتکل SET را تدوین نموده اند که از طریق بکارگیری یک تایید دیجیتالی هویت فرستنده را مورد شناسایی و تایید قرار میدهد.

کیف پول الکترونیکی
Digital Wallet

-یکی از روشهای پرداخت الکترونیکی تحت پرتکل SET میباشد. و با بکار گیری روشهای رمز نویسی Encryption ارزش مالی خریدار را برای فروشنده ارسال و حفظ مینماید.

-کیف پول دارای دو دسته نرم افزار میباشد ۱-براساس کارفرما client base ۲- بر اساس خادم Server base

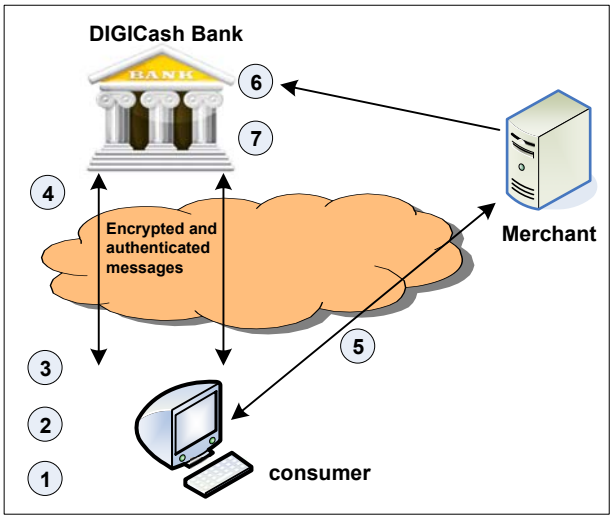
-شرکتهای Visa,MNBA از این روش استفاده میکنند.

Client base wallet: Gator,Masater Card wallet

Server base wallet: Microsoft Passport , cybercash instabuy , Novell digitalme , yodlee.com

پول نقد الکترونیکی
E-cash

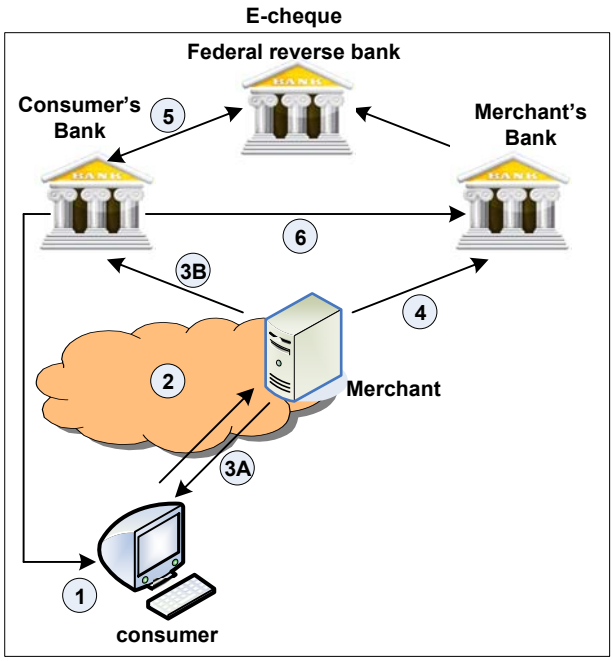
E-Cash



در این روش ارزش پولی بصورت الکترونیکی ،ذخیره سازی یا تبادل میشود که قابلیت تبدیل آن بسیار محدود بوده و نیاز به یک واسطه دارد.

1. Stablish account at bank — حسابی برای مشتری باز میشود.
2. Download digital wallet with private and public keys
دانلود نرم افزار کیف الکترونیکی حاوی کلید عمومی و خصوصی
3. Send request for e-cash coins — ارسال درخواست به بانک برای دریافت سکه الکترونیکی(اعتبار)
4. Send e-cash coins — درخواست از طریق بسته امن به دست بانک دیجیتال میرسد.
5. Spend e-cash — پرداخت پول الکترونیکی (اعتبار) به پذیرنده coins
6. Merchant transfers e-cash coins back to bank — ارسال پول در یافتی به بانک پذیرنده (مقصد)
7. Bank credits merchant's account at bank — بروز رسانی میزان اعتبار پذیرنده در بانک

چک الکترونیکی
E-Cheque



در این روش سعی شده تا با استفاده از حسابهای جاری افراد ،امکان خرید online بر قرار گردد.

1. Consumer obtains electronic checkbook from authorized bank
مصرف کننده از بانک درخواست چک الکترونیکی میکند

2. Consumer issues e-cheque to pay for purchase
مصرف کننده از طریق بستر امن اقدام به صدور چک و استفاده از آن میکند.

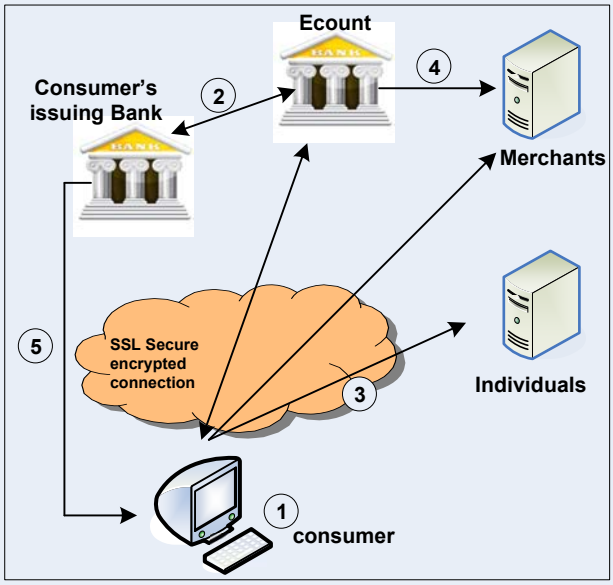
3B 3A Merchant authenticates consumer's bank & consumer ID
احراز هویت اطمینان از بانک صادر کننده و واسط از طریق استعلام

4. Merchant deposits e-cheque — پرداخت وجه چک از طریق بانک واسط به فروشنده

5. Federal reserve bank certifies public keys of banks
بانک مرکزی بعنوان متولی و استاندارد ارتباط بین بانکی ،ارتباط بین بانک واسط و پذیرنده را برقرار میکند.

6. Consumer's bank transfer funds to merchant's bank
بانک صادرکننده پرداخت را به بانک عامل انجام میدهد و صدور فاکتور برای مشتری

روش پرداخت روخط
Online payment



بعنوان سریعترین روش روی خط در اینترنت میباشد. و به کمک ذخیره سازی ارزش پولی افراد به کمک مکانیزمهایی همچون کارت هوشمند (Smart Card) انجام میگردد. مانند شرکت Ecount.com

1. Stablish account at Ecount ,founded by ceredit or debit card.
مصرف کننده یک حساب در موسسه ای مانند Ecount ایجاد میکند.

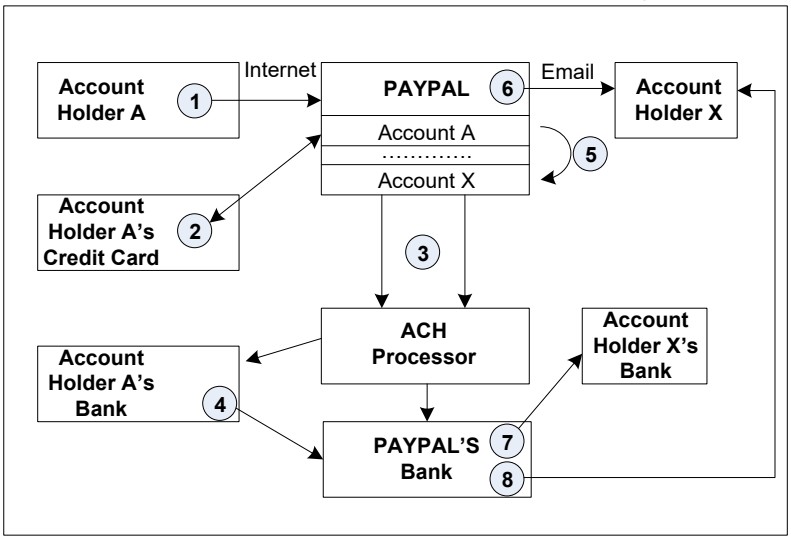
2. Verify Account And Balance. — استعلام و احراز هویت از بانک صادر کننده.

3. Makes purchases from merchants by choosing mastercard option or send cash to individuals via Email. — تاییدیه پول از طرف خریدار بصورت Email یا (حواله/اعتبار) به فرد فروشنده یا حساب فروشنده منتقل میشود.

4. Ecount transfers funds to merchant or individuals.
موسسه Ecount پول واقعی را از حساب خریدار کم و به حساب طرف مقابل (فروشنده) اضافه میکند.

5. Monthly statement issued to consumer showing debit to Ecount.
صدور صورتحساب بصورت ماهیانه از سمت بانک صادر کننده (خریدار) برای مشتری.

Email Payment (PAYPAL)



1. A pays X via PAYPAL (A has enough in PAYPAL Account)
2. Or PAYPAL Charges X's Credit Card
3. Or PAYPAL initiates ACH Debit
4. Funds are deposited in PAYPAL's Bank
5. PAYPAL credits X's PAYPAL account
6. PAYPAL notifies X of Payment and X Chooses payment method
7. Or PAYPAL initiates ACH credit
8. Or PAYPAL Mails cheque to X

Account در اینجا بمعنی شماره حساب نیست بلکه ثبت نام در سایت PAYPAL میباشد.

1. A بشرط داشتن موجودی کافی درحساب خود پول را از طریق PAYPAL پرداخت میکند.
2. یا A تمایل خود را به خرید از طریق اعتبار (کارت اعتباری) نشان میدهد.
3. پول از حساب A به صورت نقدی به حساب X واریز شود – در یک بستر امن PAYPAL ایجاد یک ارتباط بین دو بانک انجام میدهد.
4. پول از بانک A به بانک PAYPAL واریز میشود.
5. پول X نزد بانکPAYPAL به امانت میماند.(جهت افزایش اعتبار Xدر PAYPAL)
6. ارسال email ازPAYPAL به X جهت تعیین متد پرداخت.
7. یا X مجوز واریز پول بحساب خود را صادر میکند
8. یا X درخواست صدور چک از PAYPAL را اعلام میکند.

PAYPAL یکی از موفق ترین نظامهای پرداخت الکترونیکی بوده که به کمک واسطه عمل میکند.

PAYPAL در کنار نظام بانکی خود با سیستم بانکی معمولی یا سنتی نیز کار کرده و به ازای هر نقل و انتقال پولی درصدی را از مشتری اخذ میکند .

PAYPAL بعلت کار کردن آن با سیستم بانکی از درجه اطمینان بالاتری برخوردار بوده و جایگاه مهمی در اینترنت دارد.

PAYPAL برای نقل و انتقال بین المللی پول و تبادل ارزی سیستم خودش را گسترش داده و ارتباط بانک به بانک مشابه داخل امریکا در سطح بین الملل هم برقرار میباشد.

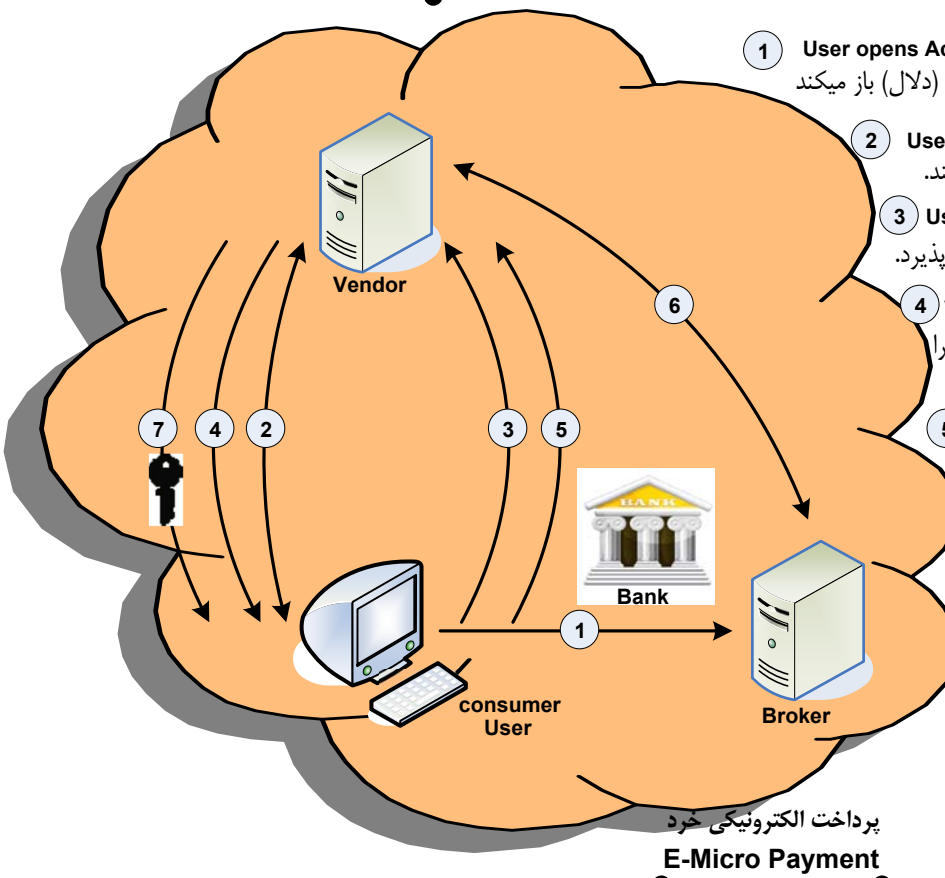
PAYPAL برای فعالیت های تجاری و نقل و انتقالات آن درصد خاصی در نظر گرفته شده ،اما برای افراد عادی ظاهرا این هزینه بصورت مجانی در نظر گرفته میشود.

PAYPAL همانند سایر بانکها ،برای سپرده ها سود در نظر گرفته و امکان جابجایی پول به کمک تلفن همراه را نیز میسر ساخته است.

کارت هوشمند آمریکایی

-موندکس یکی از منشعبات Master Card میباشد. و جهت استفاده از کارت موندکس نیاز به کارتخوان خاص موندکس میباشد (Mondex Terminal) . بنابراین هم فروشنده و هم خریدار باید دارای ترمینال مذکور باشند تا تبادل پول نمایند. با کمک موندکس از سه سنت به بالا پرداخت پول بصورت الکترونیکی ،تلفنی و یا از طریق ترمینالهای فروشگاه امکان پذیر است.

مراحل خرید محصولات توسط مستر کارت
Master Card Pre-funded to Purchase Goods



1. **User opens Account With Broker**
کاربر حسابی در نزد واسطه (دلال) باز میکند

2. **User negotiates Purchase**
کاربر خرید را آغاز میکند.

3. **User Accepts by Sending digital Signature**
کاربر با ارسال امضای الکترونیکی شرایط خرید را می پذیرد.

4. **Vendor sends Encrypted Goods**
فروشنده بصورت رمز شده نوع محصولات (خرید) را به کاربر ارسال میکند.

5. **User Sends Verification**
کاربر تاییدیه را به فروشنده ارسال میکند.

6. **Vendor Sends Verification to broker & Broker Sends Funds**
فروشنده تاییدیه کاربر را به واسطه ارسال میکند و واسطه پول را به حساب فروشنده ارسال میکند.

7. فروشنده (بازرگانی) تاییدیه جهت خرید از واسطه را برای کاربر ارسال میکند.

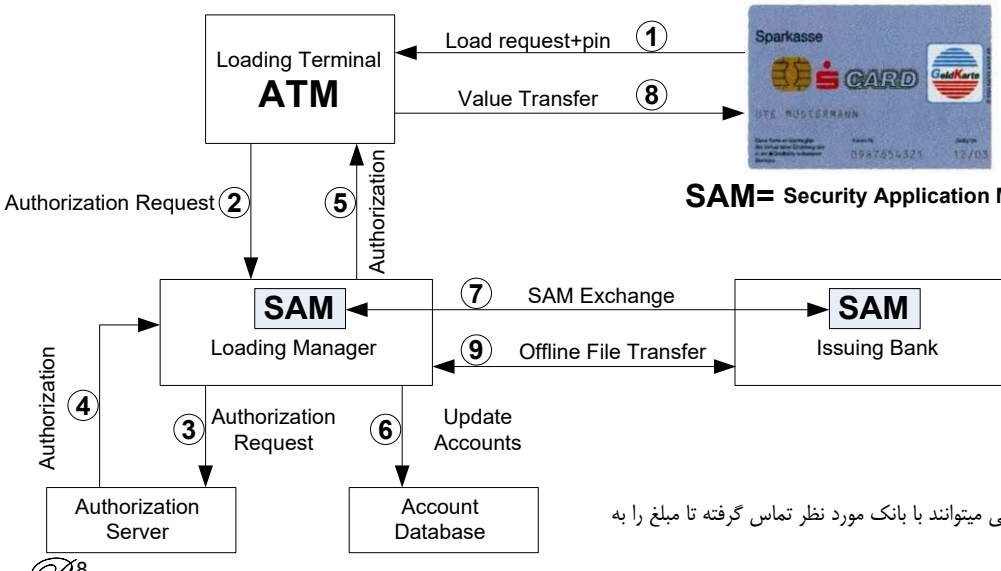
پرداخت الکترونیکی خرد
E-Micro Payment

بعلت مشکل کارت پولهای الکترونیکی که برای موارد خا (تلفن،خط اینترنت ،...)استفاده میشود ،بانکها کیف پول الکترونیک را بوجود آورده اند E-Purse تا همین کاربرد را داشته باشد.

بانک بنا به درخواست مشتری و پرداخت مبلغی که میخواهد در داخل کیف الکترونیکی اش قرار گیرد آنرا شارژ میکنند و دارنده کارت بصورت بروی خط از آن استفاده میکند.

-برای پرداختهای خرد (زیر ده دلار) استفاده میشود مانند شرکتهای Ecoin.net , Qpass.com

کارت هوشمند Geld Karte



SAM= Security Application Module

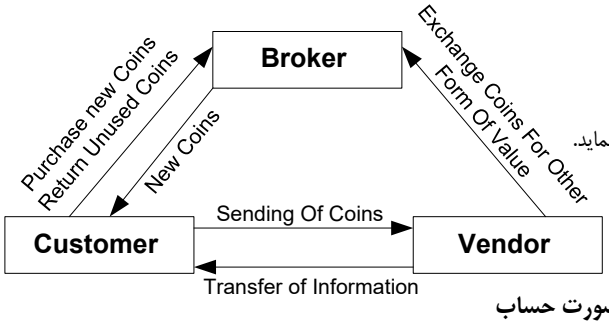
با توجه به حافظه گمارده شده در آن میتواند اطلاعات بیشتری نیز در مورد پول و مشخصات آن در بر داشته باشد.

1. بارگذاری کارت + ورود پین
2. درخواست احراز هویت
3. ارسال احراز هویت به سرور
4. پاسخ احراز هویت از سرور
5. مطلع شدن ATM از احراز هویت
6. بروز شدن حساب متری بر اساس میزان خرید
7. تبادل اطلاعات بین بانک و loading manager
8. ثبت داد وستد به داخل کارت ماژول
9. ارسال رسید خرید برای SAM بانک

فروشندگان در آخر هر روز با جمع زدن مبالغ الکترونیکی دریافتی میتوانند با بانک مورد نظر تماس گرفته تا مبلغ را به حساب آنها واریز نماید.هزینه بانک حدود 3٪ میباشد.

سکه الکترونیکی
E-Coin

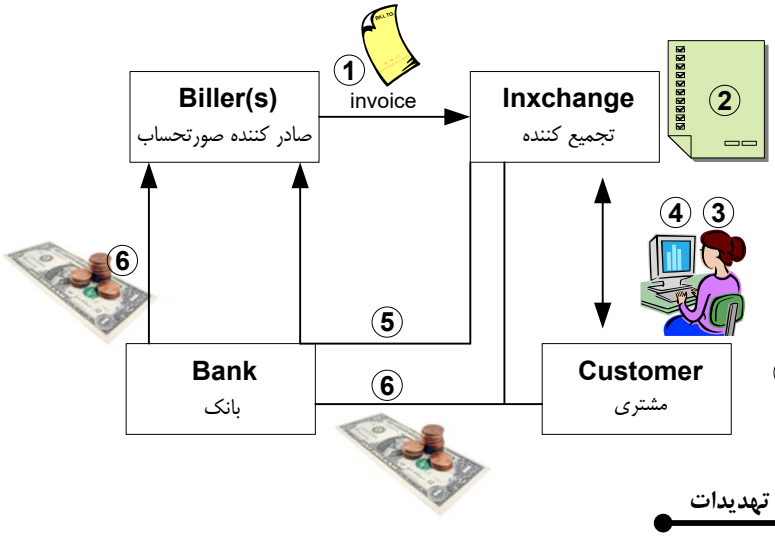
در این روش واسطه سکه های الکترونیکی را صادر وبه خریدار میفروشد سپس خریدار به کمک آنها خرید خود را انجام داده و به فروشنده پرداخت مینماید ،در نهایت فروشنده ،مبلغ معادل سکه های الکترونیکی را بصورت پول واقعی از واسطه دریافت مینماید.



1. واسطه سکه های الکترونیکی را صادر وبه خریدار میفروشد
2. خریدار به کمک آنها خرید خود را انجام داده و به فروشنده پرداخت مینماید
3. فروشنده ،مبلغ معادل سکه های الکترونیکی را بصورت پول واقعی از واسطه دریافت مینماید.

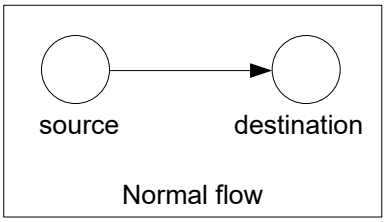
پرداخت الکترونیکی صورت حساب
Electronic Invoice Presentment and Payment (EIPP)

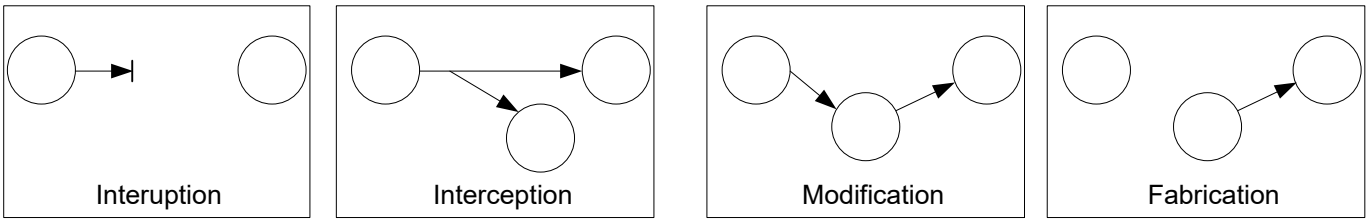
خدمات اینگونه شرکتها در شبکه اینترنت معمولا با جمع آوری صورتحسابهای حال و آینده مشتریان در سایت و صفحه مربوطه آغاز شده و مشتری متناسب بودجه نقدینگی خود ، پرداخت آنها را زمانبندی نموده و سپس از طریق بانک مشتری وجه مورد نظر در سر موعد به حساب ارسال کننده صورتحساب واریز میگردد.



1. Statement or bills rendered in electronic form on web
شرکتهای تولید کننده صورتحساب ، صورتحسابها را در وب برای شرکت واسط ارسال میکنند.
2. Multiple bills consolidated at one site
شرکت واسط تمامی صورتحسابهای یک مشتری خاص را بصورت یکجا نگهداری میکند.
3. Customer visit the site to view their bills
مشتری از طریق این واسط از صورتحسابهایش مطلع میشود.
4. Customers review bills and schedule payments
مشتری صورتحسابها را ملاحظه و اقدام به برنامه ریزی برای پرداخت میکند.
5. Remittance information returned to biller electronically
شرکت واسط برنامه ریزی پرداخت مشتری را به شرکتهای صادر کننده اطلاع میدهد.
6. Payments routed from customer's bank account to the biller's account
بانک طبق برنامه زمانبندی شده پول را برای واسط ارسال میکند.

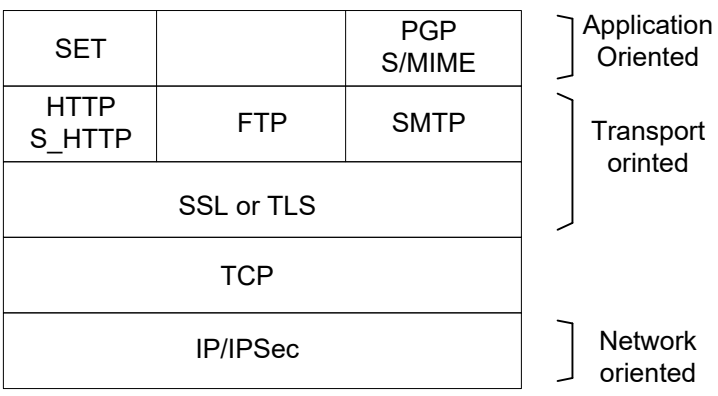
ایمنی در برابر تهدیدات





به منظور مقابله با انواع حملات فوق ،انواع سیستمهای ایمنی نیز طراحی و بکار گرفته شده که هر یک از آنها در لایه ای از کل سیستم وظیفه امنیتی را عهده دار میباشد.

انواع روشهای ایمنی و لایه های آن



راه های مقابله با حملات

-با توجه به هزینه بر بودن حملات بر اساس تحلیل و پیش بینیهای لازم میتوان احتمال حملات را تخمین زد و بر اساس آن برنامه های لازم را به اجراء در آورد.
-سرفصل سیاستگذاری امنیتی در حوزه اینترنت و مقابله با حملات در سطح جهانی با عنوان Security Policy مطرح میگردد.

بعضی از راه های برخورد با حملات

-ایجاد فایل اختصاصی برای هر کدام از کاربران و استفاده از رمز عبور
-طبقه بندی اطلاعات و نحوه دسترسی به آنها در چند لایه
-تقویت ایمنی سخت افزاری و نرم افزاری
-ایمن سازی سیستم رتباط تلفنی (Dial in)
-کشف خلاء های امنیتی سیستم و برطرف سازی آنها
-استفاده از سیستمهای دیواره آتش Firewall
-استفاده از روشهای رمز نویسی Encryption

رمزنگاری

تعریف رمز نگاری

استفاده از قوانین یا الگوریتمهای ریاضی برای پنهان سازی اطلاعات . رمز نگاری از شاخه های ریاضیات محض میباشد.

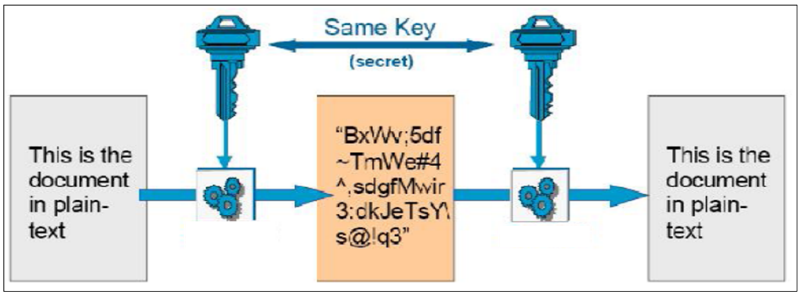
پنج عنصر هر الگوریتم

۱: پیام یا اطلاعات اولیه Plain Text
۲: پیام یا اطلاعات رمز شده Cipher Text
۳: رمز نویس (پیامهای اولیه را رمزدار میسازد) Encryptor or Encryption Algorithm
۴:کلید سری یا عامل رمز ساز Secret Key
۵: رمز گشا Decryptor or Decryption Algorithm

روشهای رمزنگاری

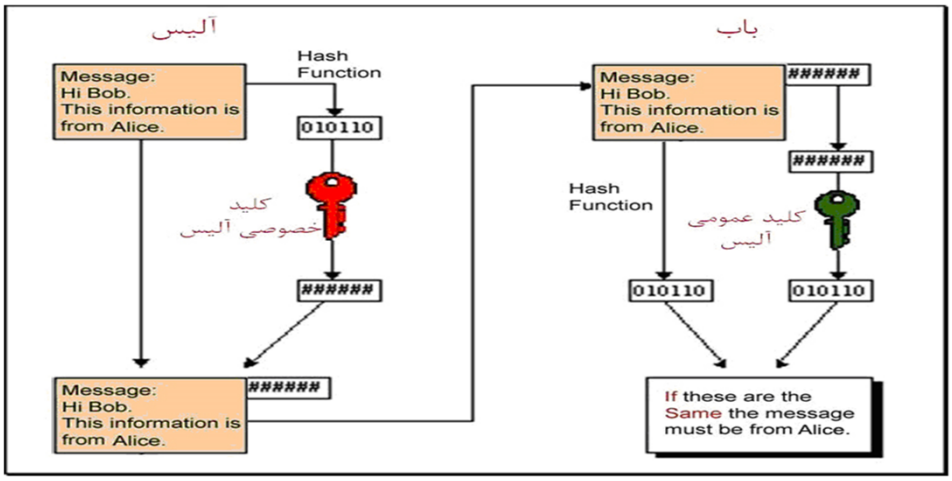
الگوریتم‌هاي متقارن
Symmetric Algorithms

-نیاز به یک الگوریتم قوی داشته
-ارسال کننده و دریافت کننده باید فرایند امنی را برای تبادل کلید فراهم سازند
-روش حمله یا بدل این روش از رمز شناسی Cryptanalysis و بکارگیری خشونت و شکنجه استفاده میشود.
-چون کلید رمز استفاده شده در طرفین یکسان میباشد لذا آنرا متقارن Symetric مینامند.
-استاندارد این روش معروف به Data Encryption Standard (DES) میباشد که بیشترین کاربرد آن ۵۶ بیتی میباشد و بصورت Triple هم استفاده میشود که ۱۶۸ بیتی میباشد.
-پیام اولیه Plain Text معمولا ۶۴ بیتی بوده و ۱۶ بار با کلید رمز که ۵۶ بیتی است ترکیب میشود
-از روش Triple بعلت بزرگ شدن بیت در آن از نظر بکارگیری در نرم افزارها با مشکل روبروست



الگوریتم‌هاي نامتقارن
روش کلید عمومی (PK)
Asymmetric Algorithms

-کلید عمومی Public Key بجای استفاده از بیتها از معادلات ریاضی استفاده کرده و از دو کلید کاملا مجزا بهره میگیرد
-این روش هم از درجه ایمنی بالایی نسبت به روش سنتی برخوردار بوده و هم بعلت عمومیت داشتن آن تقریبا جایگزین روش سنتی شده است.



الگوریتم‌هاي متقارن
Symmetric Algorithms

در رمز نگاری کلید پنهانی که به عنوان رمز نگاری متقارن شناخته می شود، از یک کلید برای رمز گذاری و رمزگشایی پیغام استفاده می شود. بنابراین فرستنده و گیرنده پیغام باید یک راز مشترک داشته باشند که آن کلید است.

یک الگوریتم مشهور رمزنگاری "استاندارد رمزگذاری داده" یا DES (Data Encryption Standard) می باشد که در مؤسسات مالی برای رمز کردن شماره هویت‌فردی یا PIN (Personal Identity Number) استفاده می شود.

کاربردهای رمزنگاری متقارن

- برای رمزگذاری حجم زیادی از اطلاعات استفاده می‌شود.
- هنگامی که همراه با گواهی الکترونیکی استفاده گردد؛ باعث حفظ محرمانگی اطلاعات است.
- زمانی که با امضاء الکترونیکی استفاده گردد؛ تمامیت پیغام را تضمین می‌نماید.

تحلیل الگوریتم‌های متقارن

مزایا

- سرعت بالا هنگام رمزگذاری
- تولید کلید به طور تصادفی و سریع

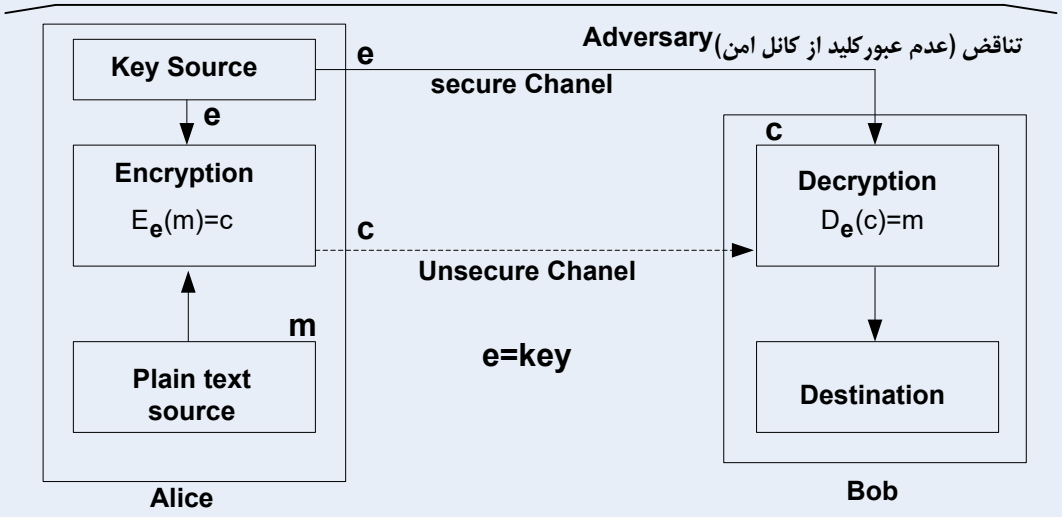
معایب

- تعدد کلیدها برای اعضای هر ارتباط
- توزیع کلید بین طرفین ارتباط

موارد استفاده

- رمزگذاری حجم زیادی از اطلاعات هنگام ذخیره روی رسانه ناامن
- رمزنگاری داده‌ها هنگام انتقال توسط رسانه ناامن

مدل رمزنگاری متقارن
Symmetric Cryptography Model



الگوریتم‌هاي نامتقارن
Asymmetric Algorithms

تحلیل الگوریتم‌های نامتقارن

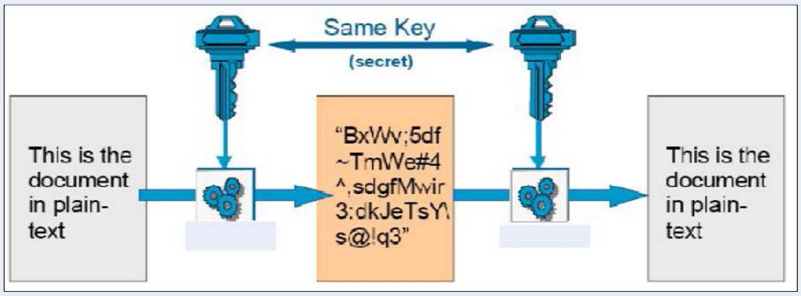
مزایا

- عدم نیاز به توزیع و ارسال کلید

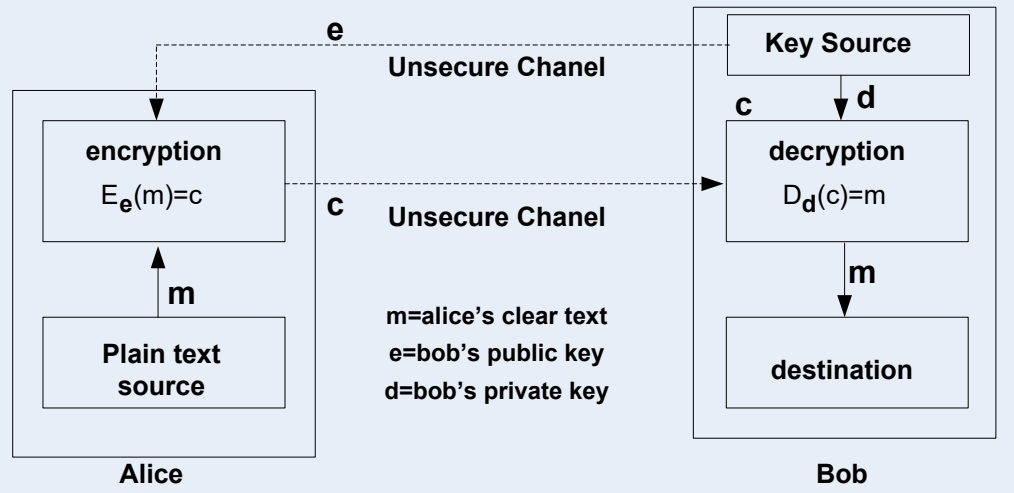
معایب

- سرعت پائین در حجم اطلاعات بالا
- پیچیدگی تولید کلید
- موارد استفاده
- در تکنولوژی امضای الکترونیکی

- برای رمز کردن داده برای هر طرف شرکت کننده فقط به کلید عمومی آن شرکت کننده نیاز است در نتیجه تنها تأیید کلید عمومی شرکت کننده ها لازم است.
- مهم ترین ویژگی های تکنیک نامتقارن غیر قابل انکار بودن، امضای الکترونیکی و تأیید منبع داده‌ای صحیح می باشد.
- در رمزنگاری نامتقارن بازرگان یک جفت کلید عمومی و خصوصی ایجاد می کند و کلید عمومی را منتشر می کند تا مصرف کنندگان از طریق آن کلید، پیغام‌هایشان را رمز کرده برای او بفرستند.
- در نهایت بازرگان به عنوان تنها دارنده کلید خصوصی، تنها کسی است که می تواند پیغام‌های رمز شده با آن کلید عمومی را باز کند.



روش توزیع کلید درمدل رمزنگاری نامتقارن
Asymmetric
Cryptography Model



توابع درهم سازی

الگوریتم‌های درهم سازی یا Hash بر خلاف دو الگوریتم ذکر شده از کلید استفاده نمی‌کنند و عمل رمزنگاری به صورت یک‌طرفه بر روی اطلاعات انجام می‌دهند. عملکرد این توابع بر روی داده‌ها بدین شکل است که با اعمال یک تابع Hash بر روی یک متن، یک چکیده یا دایجست از متن بدست می‌آید.

- فرآیندی است که بصورت ریاضی حجم یک جریان از داده را به یک طول ثابت کاهش می دهد.)معمولا ۱۲۸ و یا ۱۶۰ بیت(
- عملکرد hash مشابه اثرانگشت یک شخص می باشد.
- اثرانگشت، پارامتری منحصر بفرد به منظور تشخیص هویت افراد بوده و در ادامه با استفاده از آن امکان دستیابی به سایر مشخصات افراد نظیر: رنگ چشم، قد، جنسیت و سایر موارد دلخواه، فراهم می گردد.

ویژگی های توابع درهم سازی

- امکان استنتاج ورودی از طریق خروجی وجود ندارد.
- نمی توان دو ورودی را پیدا کرد که به ازای آنان خروجی یکسانی تولید گردد.

تحلیل توابع درهم سازی

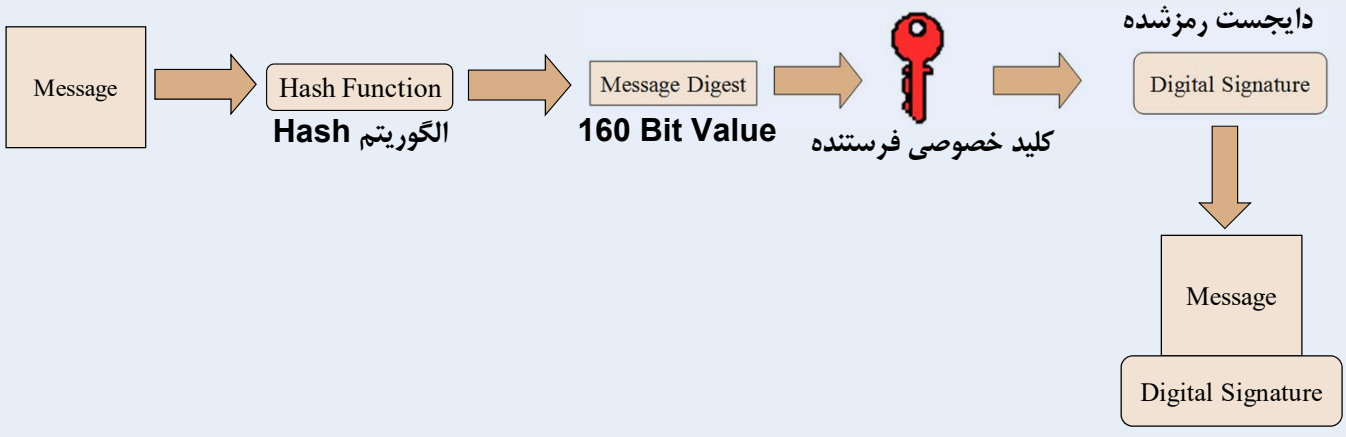
مزایا

•عدم نیاز به تولید و ارسال کلید
•سرعت بسیار بالا

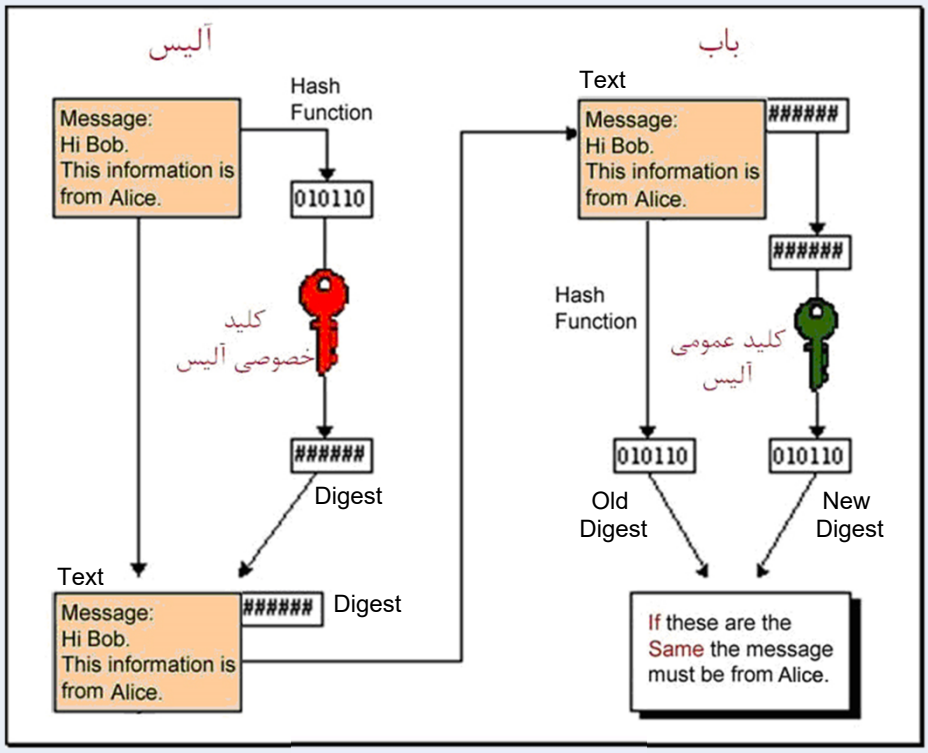
موارد استفاده

•تضمین تمامیت پیغام

نحوه امضاء یک پیغام الکترونیکی



اعتبارسنجی امضای الکترونیکی



امضاء الکترونیکی و محرمانگی