امنیت تجارت الکترونیک

جلسه چهارم:
سیستم های پرداخت الکترونیکی

تهیه و تنظیم: دکتر آرش حبیبی لشکری

اولین نسخه: دی 1393
بروزرسانی: شهریور 1394

فهرست:

- **سیستم های پرداخت الکترونیکی**
  - آنلاین - آفلاین
  - بدهکاری (Debit) در برابر اعتبار(Credit)
  - خرد (Micro) در برابر کلان (Macro)
- **ابزارهای پرداخت**
  - کارتهای اعتباری
  - پول الکترونیکی
  - چک الکترونیکی
  - کیف پول الکترونیکی
  - کارتهای هوشمند
- **مشکلات امنیتی پرداخت**
  - مشکلات امنیتی پرداختهای سنتی و الکترونیک
  - نیازمندیهای امنیتی

سیستمهای پرداخت الکترونیک

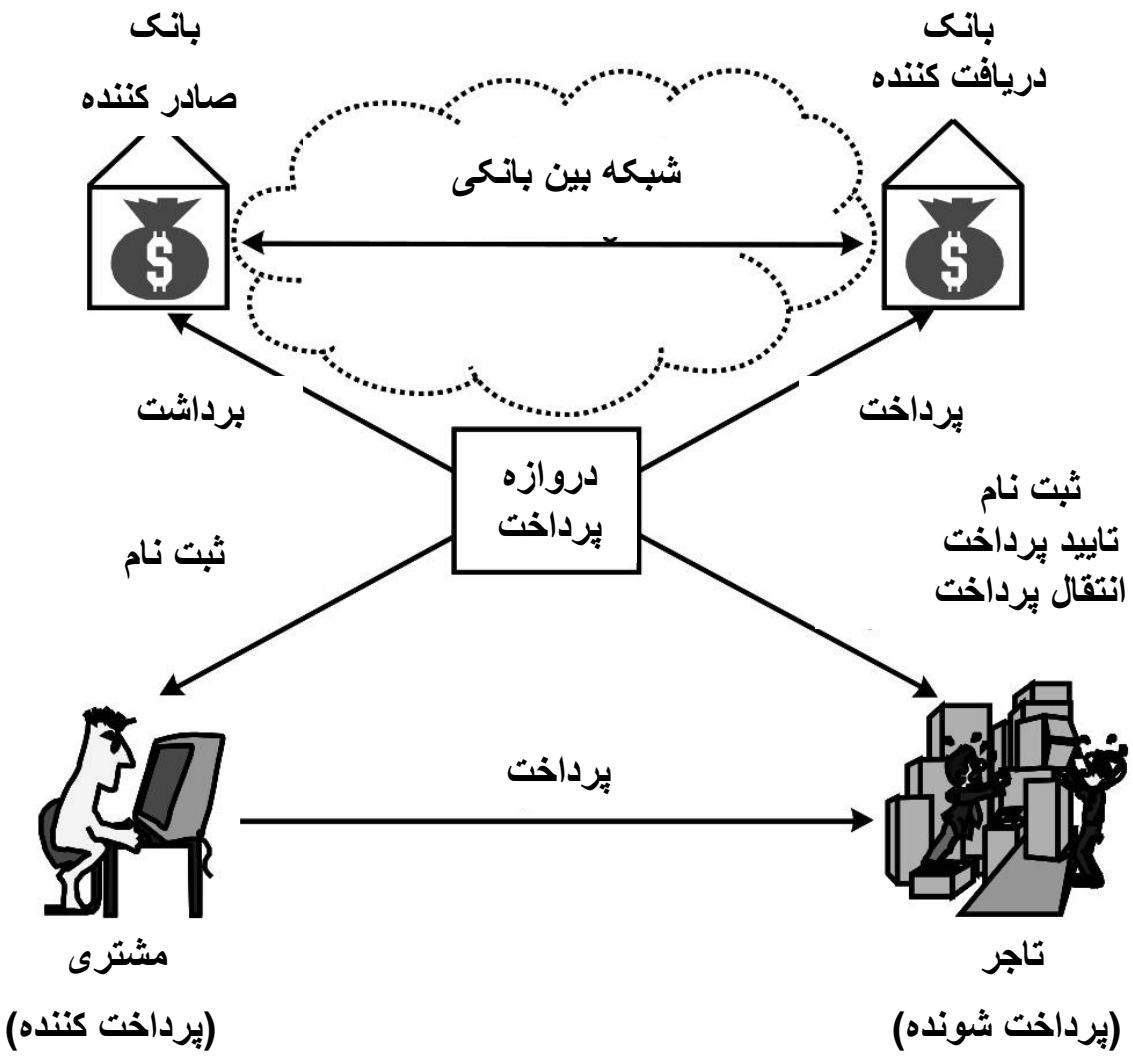
سیستمهای پرداخت الکترونیک

- قبل از طراحی یک سیاست امنیتی:
  شناخت کاملی از سیستم
  و خطراتی که سیستم را تهدید میکنند

- تجارت الکترونیک (یا E-Commerce) به تمامی تراکنشهایی گفته میشود که دربر گیرنده چندین تبادل ارزشمند (مالی) روی شبکه های ارتباطی می باشند. این تعریف وسیع شامل:
- تراکنشهای شرکت به شرکت، از قبیل تبادلات داده الکترونیکی (EDI)
- تراکنشهای مشتری به شرکت، از قبیل فروشگاه های الکترونیک در وب
- تراکنشهای مشتری به مشتری، از قبیل انتقال پول بین کیف پولهای الکترونیکی
- تراکنشهای مدیریتی مشتری یا شرکت به مردم، از قبیل پرکردن فرمهای الکترونیک اظهار نامه های مالیاتی

به هر نوع سرویس شبکه ای که شامل تبادلات مالی برای کالاها یا سرویسها باشد، یک سیستم پرداخت الکترونیک اطلاق میشود

سیستم پرداخت الکترونیک



سیستم پرداخت الکترونیک

به منظور شرکت در یک سیستم پرداخت الکترونیک، یک مشتری و فروشنده باید به‌اینترنت دسترسی داشته و می بایست از قبل خود را در سیستم ارائه دهنده سرویس پرداخت ثبت نمایند.

ارائه دهنده سرویس یک پورت پرداخت راه‌اندازی می نماید، که هم از شبکه عمومی (مثل‌اینترنت) قابل دسترسی بوده و هم از شبکه مختص به نقل و انتقالات بانکی دسترس پذیر باشد.

پورت پرداخت نقش یک واسط بین زیرساخت پرداخت سنتی و زیرساخت پرداخت الکترونیک را ایفا می نماید. یکی دیگر از پیش نیازها، داشتن یک حساب بانکی برای مشتری و فروشنده است که به شبکه نقل و انتقالات بانکی متصل باشد. بانک مشتری معروف به بانک صادر کننده است.

عبارت بانک صادر کننده در واقع بانکی است که ابزار پرداخت (مانند کارت اعتباری) را مهیا می نماید که مشتری برای پرداخت از آنها استفاده می کند. بانک دریافت کننده نیز تاریخ پرداختها را (یا بصورت کاغذی و یا به صورت داده‌های الکترونیک) از طرف فروشنده دریافت می کند.

سیستم پرداخت الکترونیک

در زمان خرید کالا یا سرویس ها، مشتری (یا پرداخت کننده) مقداری پول به تاجر (یا پرداخت شونده) پرداخت می کند. فرض کنیم که مشتری بخواهد با کارت اعتباری خرید را انجام دهد. قبل از تامین کالاها و سرویس ها سفارش داده شده، تاجر از پورت پرداخت درخواست مجوز برای پرداخت کننده و همچنین برای ابزار پرداخت خود می کند.

پورت پرداخت با بانک صادر کننده برای بررسی صدور مجوز تماس می گیرد. اگر همه چیز به درستی انجام شود، مقدار پول موردنظر از حساب مشتری دریافت شده (یا مشتری به بانک خودش بدهکار میشود) و به حساب تاجر منتقل میشود. این پردازش نشانگر تراکنش پرداخت واقعی است.

پورت پرداخت خبر موفقیت تراکنشهای پرداخت را به تاجر می دهد، بنابراین تاجر موارد سفارش داده شده توسط مشتری را تامین میکند. در برخی موارد، مخصوصا وقتی سرویسهای کم هزینه سفارش داده می شوند، اقلام و کالاها می توانند قبل از صدور مجوز پرداخت و تراکنش هزینه، تحویل مشتری داده شوند.

آنلاین در برابر آفلاین

یک سیستم پرداخت الکترونیک میتواند هم آنلاین و هم آفلاین باشد.

در یک سیستم آفلاین، پرداخت کننده و پرداخت شونده در زمان انجام تراکنش پرداخت برای یکدیگر، آنلاین هستند، ولی هیچ ارتباط الکترونیکی مابین بانکهای آنها وجود ندارد. دراین سناریو، دریافت کننده امکانی برای درخواست مجوز از بانک صادر کننده (از طریق پورت پرداخت) ندارد، بنابراین نمیتواند از دریافت پول اطمینان حاصل نماید. پس دراین حالت جلوگیری از اینکه پرداخت کننده بدون داشتن مجوز، بیشتر از مقدار دارایی خود خرج کند، امکان پذیر نخواهد بود.

اصولا به‌این دلیل است که، اکثر سیستمهای پرداخت اینترنتی ارائه شده امروزه آنلاین هستند.

یک سیستم آنلاین نیازمند وجود یک سرور صدور مجوز آنلاین است، که می تواند بخشی از بانک صادرکننده یا دریافت کننده باشد. واضح است که یک سیستم آنلاین نیازمند ارتباطات بیشتری است ولی‌ایمن تر از سیستمهای آفلاین خواهد بود.

بدهکاری (Debit) در برابر اعتبار(Credit)
خرد(Micro) در برابر کلان (Macro)

یک سیستم پرداخت الکترونیک می تواند بر اساس بدهکاری یا اعتباری بنا نهاده شده باشد. در یک سیستم اعتباری (مثل کارتهای اعتباری) مبالغ پولی در حساب پرداخت کننده سپرده میشود. سپس پرداخت کننده مجموع مقادیر را به سرویس پرداخت می پردازد. در یک سیستم بدهکاری (مثل چک و کارتهای Debit) حساب پرداخت کننده به محض‌اینکه تراکنش پردازش شد، بدهکار میشود.

یک سیستم پرداخت الکترونیک که قابلیت تبادل مقادیر زیاد پولی را دارد به سیستم پرداخت کلان معروف است. از طرف دیگر، اگر یک سیستم برای پرداختهایی با مقادیر کم (مانند تا 5 یورو) باشد، به سیستمهای پرداخت خرد معروف میباشد. اندازه مقادیر جابجا شده، نقش مهمی‌در طراحی سیستم و تصمیم گیری روی سیاستهای امنیتی آنها بازی میکند. پیاده سازی پروتکلهای امنیتی گران برای محافظت از سکه‌های دیجیتال با مقادیر کم بی معنی است. دراین موارد جلوگیری از حملات بزرگ که تعداد بسیار زیادی از سکه‌های دیجیتال را جعل کرده یا می ربایند، بسیار حائز اهمیت خواهند بود.

ابزارهای پرداخت

ابزارهای پرداخت

ابزارهای پرداخت وسیله هایی برای پرداخت می‌باشند.

پول کاغذی، کارتهای اعتباری و چکها ابزارهای سنتی پرداخت میباشند و ابزارهای جدید پرداخت الکترونیکی عبارتند از: پول الکترونیک (پول دیجیتال) و چکهای الکترونیک. همانطور که این اسامی خود بیانگر مفهوم خاصی هستند، اینها در اصل الگوهای جدیدی نیستند، بلکه صورت الکترونیکی ابزارهای پرداخت سنتی میباشند. هرچند،این موارد جدید از جنبه های مختلفی نسبت به پیشینیان خود تفاوت دارند ولی به طور مشترک در همه ابزارهای پرداخت، چرخه پول از حساب پرداخت کننده به حساب پرداخت شونده خواهد بود.

ابزارهای پرداخت : سیستمهای پرداخت نقد - مانند و سیستمهای پرداخت چک – مانند

در یک سیستم نقد- مانند، پرداخت کننده از حسابش مقدار مشخصی پول (پول کاغذی، پول الکترونیکی) برداشت میکند و در زمانی که میخواهد پرداختی انجام دهد از آن استفاده میکند.

در یک سیستم چک- مانند، پول در حساب کاربر باقی میماند تا وقتی که خریدی انجام شود. پرداخت کننده، یک سفارش پرداخت به پرداخت شونده ارسال میکند، براین اساس که پول از حساب پرداخت کننده برداشت شده و به حساب پرداخت شونده واریز خواهد شد. سفارش پرداخت می‌تواند یک سند کاغذی (مانند برگه انتقال بانکی) یا یک سند الکترونیکی (مانند یک چک الکترونیکی) باشد. سه بخش بعدی، مروری بر تراکنشهای پرداختی دارند که با ابزارهای پرداخت متفاوتی سروکار خواهند داشت.

کارتهای اعتباری

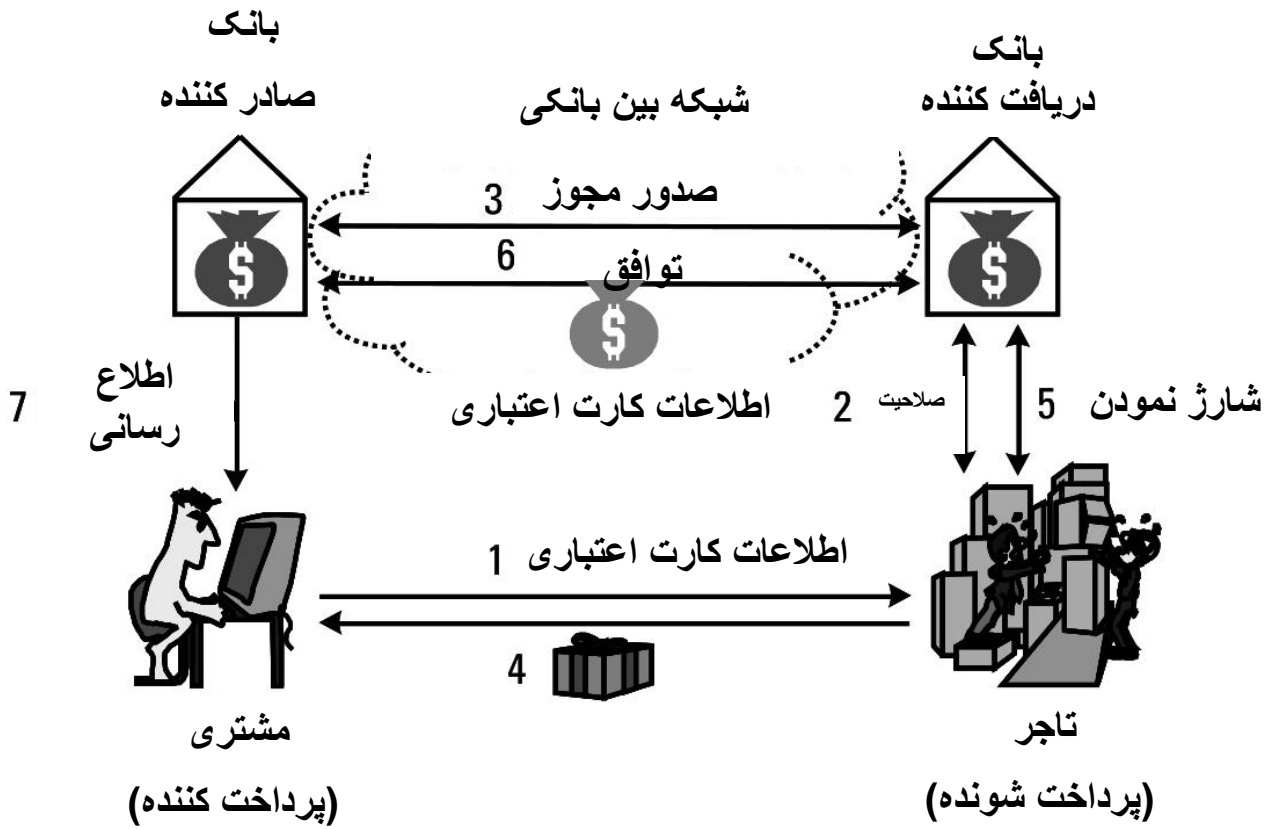
برخی از سیستمهای پرداخت الکترونیک از ابزارهای پرداخت سنتی استفاده میکنند. برای مثال در حال حاظر کارتهای اعتباری، محبوب ترین ابزار پرداخت دراینترنت میباشند. اولین کارتهای اعتباری دهه ها قبل (Diner's Clubدر سال 1949، American Expressدر سال 1958) معرفی شدند.

برای مدتهای زیادی، کارتهای اعتباری با نوارهای مغناطیسی، حاوی اطلاعات رمزگذاری نشده و فقط قابل خواندن، تولید می شدند. امروزه، (کارتهای بیشتری) "کارتهای هوشمند" حاوی قطعات سخت افزاری (تراشه ها) بوده و ظرفیتهای بالایی دارند و همچنین امکان رمزنگاری در آنها نیز فراهم شده است.

به تازگی حتی کارتهای اعتباری مجازی (کیف پولهای الکترونیکی نرم افزاری)، از قبیل کارتهای شرکت Trintech Cable & Wireless نیز به بازار عرضه شده اند.

شکل بعدی یک تراکنش پرداخت معمولی که با ابزار پرداخت، کارت اعتباری انجام شده را به تصویر می کشد.

کارتهای اعتباری



کارتهای اعتباری

مشتری اطلاعات کارت اعتباری (صادر کننده، تاریخ انقصا، شماره) خود را به فروشنده می دهد (1).

فروشنده از بانک گیرنده وجه درخواست مجوز می کند (2).

بانک دریافت کننده پیامی‌از طریق شبکه بین بانکی به بانک صادر کننده، مبنی بر درخواست مجوز ارسال میکند (3).

بانک صادر کننده پاسخ درخواست مجوز را برمی گرداند (3).

اگر پاسخ مثبت باشد، بانک صادر کننده، فروشنده را مطلع میسازد که مبلغ تایید شده است. حال فروشنده میتواند کالاها و سرویسهای سفارش داده شده را برای مشتری ارسال کند (4)

مبلغ (دسته‌ای از مبالغ که نشانگر مجموعه‌ای از تراکنشها می باشد) را به بانک دریافت کننده انتقال دهد (5بالا)

بانک دریافت کننده یک درخواست تسویه حساب به بانک صادر کننده میفرستد (6به سمت چپ). بانک صادر کننده، پول را در یک حساب تسویه بین بانکی (6به سمت راست) قرار داده و از مجموع دریافتیهای موجود در کارت اعتباری مشتری، مقدار مورد نظر را اخذ میکند.

در فواصل معین (مثلا، هر ماه) بانک صادر کننده مشتری را از مجموع تراکنشهای انجام شده مطلع میسازد (7). مشتری مقادیر قابل پرداخت را از راه های مختلفی (از قبیل سفارش مستقیم کارتهای debit، انتقال بانکی، چک) میتواند به بانک بپردازد.

در همین حین، بانک گیرنده، مقدار وجه مورد نظر را از حساب تسویه بین بانکی دریافت کرده و به حساب فروشنده واریز مینماید (5پایین).

ضرورت حفاظت از محرمانگی داده های تراکنشهای پرداخت ناشی از مواردی بود که شماره های کارتهای اعتباری دزدیده شده بود.

کارتهای اعتباری

در کل، استفاده ی متغلبانه از شماره های کارتهای اعتباری از دو منبع نشات می گیرد: استراق سمع کنندگان و فروشندگان فریبکار.

شماره های کارتهای اعتباری باید در برابر موارد زیر محافظت شوند:

- استراق سمع کنندگان توسط رمزنگاری (برای مثال، SSL)
- فروشندگان فریبکار بوسیله اسامی مستعار برای شماره های کارتهای اعتباری
- هر دو مورد استراق‌سمع کنندگان و فروشندگان فریبکار توسط رمزنگاری و امضاهای دوتایی

پول الکترونیکی

پول الکترونیک شکل الکترونیکی پول سنتی است. سکه دیجیتال یا سکه الکترونیکی به یک واحد از پول الکترونیک اطلاق میشود.

در بحث پیش رو، ارزش واقعی یک سکه دیجیتال با واحدهای پول سنتی نامربوط اند. سکه های دیجیتال توسط واسطها یا همان دلالها ضرب میشوند. اگر یک مشتری بخواهد سکه دیجیتال بخرد، با یک واسط تماس میگیرد، مقداری سکه سفارش میدهد، و هزینه آن را با پول واقعی پرداخت میکند.

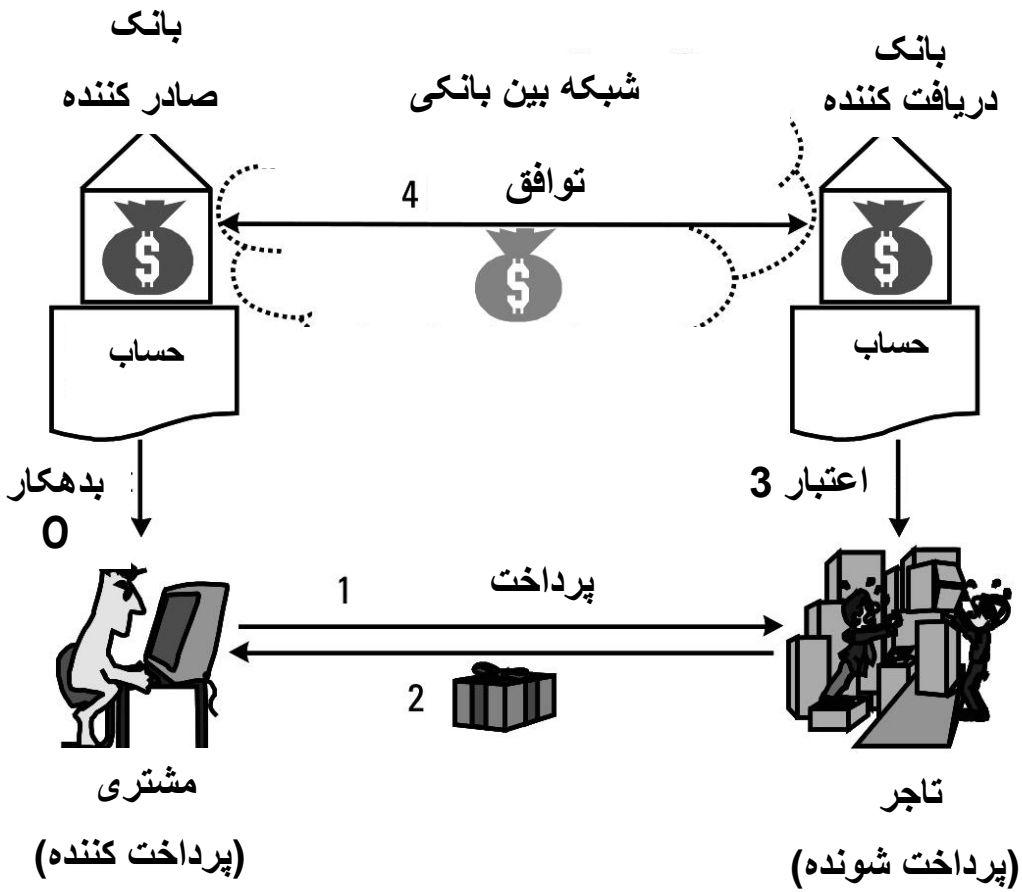
بعد از آن مشتری میتواند از هر فروشنده ای که سکه دیجیتال مربوط به آن واسط را قبول میکند، خرید نماید. سکه های بدست آمده از مشتری ها نزد هر فروشنده، می توانند توسط واسطها باز خرید شوند. به عبارت دیگر، واسط سکه ها را پس گرفته و در عوض برابر با ارزش سکه ها پول "واقعی" به حساب فروشنده واریز مینماید

پول الکترونیکی

شکل بعدی یک تراکنش معمولی پول الکترونیک را به تصویر کشیده است.

دراین مثال، بانک صادر کننده میتواند نقش واسط را ایفا نماید. مشتری و فروشنده میبایست یک حساب جاری داشته باشند. وجود حساب جاری در نقش تبدیل کننده پول حقیقی به پول الکترونیک، حداقل تا زمانی که پول الکترونیک به صورت بین المللی به عنوان یک پول رایج شناخته نشده، لازم و ضروری است. وقتی مشتریها سکه‌های دیجیتال خریداری میکنند، حساب جاری آن شخص بدهکار میشود (0). حال آن شخص میتواند از سکه ها برای خرید دراینترنت استفاده نماید (1). از آنجاییکه سکه های الکترونیک اغلب برای خرید سرویس ها و کالاهای کم ارزش استفاده میشوند، فروشندگان معمولا سفارشات مشتریان را قبل از و یا بدون درخواست هر نوع مجوز پرداخت، ارسال مینمایند. فروشنده برای بانک دریافت کننده درخواست بازخرید ارسال میکند (2). با استفاده از یک مکانیزم تسویه حساب بین بانکی، بانک گیرنده سکه ها را در برابر پول حقیقی آنها به بانک صادر کننده میدهد (3) و پول واقعی فروشنده را که معادل تعداد سکه ها است به حساب فروشنده واریز مینماید.

پول الکترونیکی



چک الکترونیکی

چکهای الکترونیک معادل الکترونیکی چکهای کاغذی سنتی هستند. یک چک الکترونیک، یک سند الکترونیکی است که حاوی داده های زیر میباشد:

شماره چک

نام پرداخت کننده

شماره حساب پرداخت کننده و نام بانک

نام پرداخت شونده

مبلغی که باید پرداخت شود

واحد پول استفاده شده

تاریخ انقضا

امضای دیجیتال پرداخت کننده

تاییدیه الکترونیکی پرداخت شونده

چک الکترونیکی

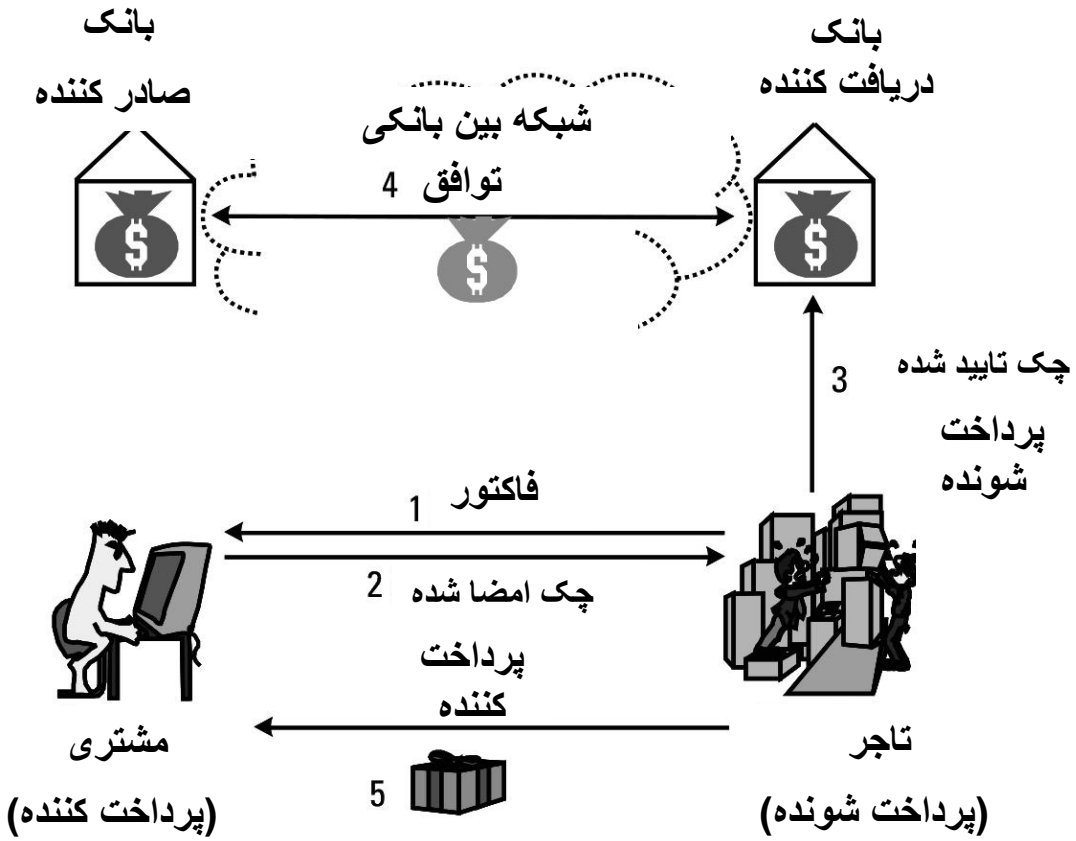
مشتری کالا و سرویس هایی را به فروشنده سفارش میدهد، که در نتیجه آن فروشنده یک صورت حساب الکترونیکی به مشتری میفرستد (1).

برای پرداخت، مشتری یک چک الکترونیک امضا شده به صورت الکترونیکی ارسال مینماید (2). (امضای الکترونیک یک عبارت کلی است که میتواند، یک امضا دیجیتال بر اساس رمزنگاری کلید عشمومی‌باشد).

در چکهای کاغذی، فروشنده مکلف به تایید چک میباشد (مثل پشت نویسی و امضای چک) (3). (تاییدیه الکترونیک نوعی از امضا الکترونیک است)

بانک صادر کننده و بانک دریافت کننده بر برداشت پول از حساب مشتری و واریز آن به حساب تاجر نظارت میکنند. بعد از دریافت چک از مشتری، تاجر باید کالاهای سفارش داده شده را ارسال نموده و سرویسهای مورد نظر را ارائه دهد.

چک الکترونیکی



کیف پول الکترونیکی

کیفهای پول الکترونیک دستگاه های سخت افزاری یا نرم افزاری می باشند که مقادیری در آنها ذخیره شده است.

مقادیر داخل آنها را می توان از طریق افزایش شمارنده پول در آنها و یا بوسیله رشته های بیتی قوی که نشان دهنده سکه های الکترونیک هستند، افزایش داد. امروزه تکنولوژی بیشتر تمایل به تولید کیفهای پول الکترونیک در تکنولوژی کارت هوشمند دارد.

در سیستم پرداخت الکترونیک که در پروژه CAFE توسعه داده شد (دسترسی شرطی برای اروپا، که توسط انجمن اروپایی برنامه ESPRIT پشتیبانی مالی شده است)، کیف پول الکترونیک هم میتواند در تصویر یک کامپیوتر قابل حمل کوچک با یک منبع تغذیه داخلی (کیف پول T) یا به تصویر کارت هوشمند (کیف پول آلفا) باشد. پول الکترونیکی را میتوان به راحتی به کیف پولهای آنلاین واریز نموده و برای پرداخت از آنها در پایانه های فروش استفاده نمود.

کارتهای هوشمند

یک کارت هوشمند یک کارت پلاستیکی است که شامل یک پردازنده جاسازی شده و یک حافظه است.

همانند کیفهای پول الکترونیکی، کارتهای هوشمند نیز قطعات سخت افزاری جدید و یک گره ارتباطی برای سیستم پرداخت معرفی میکنند. از دیدگاه واژه شناسی پرداخت، کارتهای هوشمند دراصل ارائه دهنده یک تکنولوژی هستند نه یک ابزار پرداخت جدید. به عبارت دیگر، کارتهای هوشمند میتوانند هم به عنوان کارت اعتباری و هم به عنوان منبع ذخیره پول الکترونیکی و همچنین به عنوان دستگاه های چکهای الکترونیکی یا ترکیبی از همه آنها استفاده شوند.

طی‌این سالها، کیف پولهای الکترونیکی برپایه- کارتهای هوشمند، که قابلیت شارژ مجدد دارند، بیشتر برای پرداختهای کوچک، مورد استفاده قرار میگرفتند. حساب صاحب کیف پول پیش ازاینکه خریدی انجام شود بدهکار است. صاحب کارت میتواند کارت را در یک دستگاه ATM بارگذاری نماید. فروشگاه هایی که‌این نوع پرداخت را قبول میکنند باید در قسمت صندوق به دستگاه های کارت خوان مجهز شوند. نمونه هایی مانند Austrian Quick و Belgian Proton دراین زمینه وجود دارند.

مشکلات امنیتی پرداخت سنتی و الکترونیک

مشکلات امنیتی پرداخت الکترونیک

مشکلات امنیتی سیستمهای پرداخت سنتی شناخته شده‌اند:

- پول قابل جعل است
- امضاءها قابل جعل هستند
- چکها میتوانند وصول نشده و برگشت داده شوند

سیستمهای پرداخت الکترونیک نیز همان مشکلات سیستمهای سنتی را دارند، و البته شاید هم بیشتر:

- اسناد دیجیتال کاملا و به دلخواه قابل کپی برداری میباشند.
- امضاءهای دیجیتال توسط هرکسی که کلید خصوصی را داشته باشد قابل تولید هستند.
- شناسه‌ی یک پرداخت کننده ممکن است مربوط به هر یک از تراکنشهای پرداخت باشد.

مشکلات امنیتی پرداخت الکترونیک (ادامه)

در یک سیستم پرداخت الکترونیک :

- افراد خارج ارتباط، خط ارتباطی را استراق سمع کرده و از داده های جمع آوری شده سوء استفاده میکنند (مثل شماره های کارتهای اعتباری)
- مهاجمین برای جلوگیری از فعالیت سیستم یا ربودن دارایی های رد و بدل شده، توسط حملات فعال پیامهای ساختگی به شرکت کنندگان مجازسیستمهای پرداخت می فرستند
- شرکت کنندگان سیستمهای پرداخت فریبکار سعی بر بدست آوردن و سوء استفاده از داده های تراکنشهای پرداختی دارند که مجاز به دیدن آنها نیستند.

نیازمندیهای اساسی امنیتی برای سیستمهای پرداخت الکترونیک:

- تایید اعتبار پرداخت
- یکپارچگی پرداخت
- مجوز دهی پرداخت
- محرمانگی پرداخت

نیازمندیهای امنیتی

تایید اعتبار پرداخت: دلالت بر این دارد که هم پرداخت کننده و هم دریافت کننده باید شناسه های پرداخت خود را اعلام کنند، که لزوما برابر با شناسه واقعی آنها نیست. اگر نیاز به گمنامی نباشد، یکی از مکانیزمهای تایید اعتبار پایه حوزه امنیت (جلسه اول) میتواند برای پاسخ به این نیازمندی استفاده شود. در غیر اینصورت به مکانیز خاص نیاز خواهیم داشت.

یکپارچگی پرداخت: نیازمند این است که کسی نتواند بدون مجوز داده های تراکنشهای پرداخت شامل شناسه پرداخت کننده، شناسه دریافت کننده، محتوای خرید، مقدار یا شاید اطلاعات دیگر را تغییر دهد. برای این منظور یک مکانیزم یکپارچگی پایه از حوزه امنیت اطلاعات (جلسه اول) می تواند به کار گرفته شود.

مجوز دهی پرداخت: یعنی اینکه هیچ پولی نمیتواند از حساب یا کارت هوشمند مشتری، بدون اجازه او برداشته شود و همچنین معنی دیگر آن این است که مقادیر مجاز فقط توسط اشخاص مجاز قابل برداشت هستند. برای این منظور یک مکانیزم کنترل دسترسی پایه از حوزه امنیت اطلاعات (جلسه اول) می تواند به کار گرفته شود.

محرمانگی پرداخت: پوشش دهندهی محرمانگی یک یا چند بخش از دادههای تراکنشهای پرداخت می-باشد. در ساده ترین حالت یک مکانیزم محرمانگی پایه در حوزه امنیت اطلاعات (جلسه اول) می تواند به کار گرفته شود. درمواردی که نیاز به حفاظت بخشهای مختلف از شرکت کنندگان در یک تراکنش پرداخت باشد، مکانیزمهای خاص استفاده نمود.

خلاصه:

سیستمهای پرداخت الکترونیکی، ابزار پرداخت، کارتهای اعتباری، پول الکترونیکی، چک الکترونیکی، کیف پول الکترونیکی، کارتهای هوشمند، مشکلات امنیتی پرداخت، مشکلات امنیتی پرداختهای سنتی و الکترونیک، نیازمندیهای امنیتی، سرویسهای امنیتی پرداخت،

جلسه بعدی:
سرویسهای امنیتی پرداخت

هیچ راهی برای به دست آوردن تجربه به جز از
طریق تجربه وجود ندارد.