طراحی و پیاده‌سازی

سیستم چک الکترونیکی در ایران

فریا نصیری مفخّم

سازمان انتشارات جهاد دانشگاهی
۱۳۸۴

بسم‌الله الرحمن الرحیم

فهرست مطالب

سخن ناشر

فعال سازی ظرفیت‌های موجود دانشجویی در کلیه سطوح برای تولید و انتشار آثار علمی، فرهنگی کمترین وظیفه‌ای است که ما در قبال جمعیت عظیم دانشجویان کشور برعهده داریم.

لذا در چارچوب تدابیر و طرح‌های ویژه، دبیرخانه انتخاب پایان نامه سال دانشجویی با هدف بهره‌گیری هرچه بیشتر جامعه از ظرفیت‌های علمی، فرهنگی این عرصه و نیز به منظور تعمیق، توسعه و ترویج نتایج یافته‌های دانشجویی، طرح انتشار پایان نامه‌های برتر دانشجویی را در دستور کار خود قرار داده‌است.

لذا در همین راستا و به منظور ارتباط و تعامل هرچه بیشتر جامعه با ظرفیت‌ها، قابلیت‌ها و استعدادهای دانشجویی کشور و همچنین حمایت از پایان نامه‌های برگزیده دوره هشتم، این آثار بصورت کتاب منتشر می‌شوند.

اینک که جامعه ما در آستانه خیزش بزرگ علمی است، توسعه علمی، پژوهشی و رونق آموزش عالی به یک جنبش فراگیر تبدیل شده و این نشانه بسیار خوبی از تحولات آینده در کشور است. از سوی دیگر در نیم قرن گذشته با تحولات فکری در کل جامعه جهانی مواجه بوده‌ایم.که باید بکوشیم ضمن درک عمیق این تحولات، زمینه را برای رشد و پویایی هرچه بیشتر فرهنگ ایرانی و اسلامی مهیا کنیم.

زمانی محور اصلی فعالیت‌ها در دانشگاه‌ها، آموزش بود. اما امروز با احساس ضرورت، انجام و رونق پژوهش در کشور تحولات وسیعی را به وجود آورده‌است. آمارهای موجود امیدهای تازه‌ای را ایجاد کرده‌است: از جمله آمار وجود حدود ۷۰۰ محقق در یک میلیون نفر جمعیت، که در برنامه چهارم توسعه، این رقم ارتقاء می‌یابد. همچنین مراکز پژوهشی خصوصی که در گذشته اهمیتی برای پژوهش قائل نبودند امروز در تولید علم و دانش حرف‌های زیادی برای گفتن دارند. زمینه توسعه ارتباط دانشگاه‌ها با جامعه بیشتر فراهم شده‌است بطوری که امروز شاهد اتفاقات تازه در این عرصه هستیم. دانشگاهیان ایرانی وارد عرصه‌های بین‌المللی شده‌اند، مقالات آنها در کنفرانس‌های بین‌المللی ارائه می‌شود و هر روز شاهد افزایش ارجاع به مقالات دانشمندان ایرانی هستیم که این خود نشانگر کیفیت بالای تحقیقات است با استقرار توسعه علمی در کشور، ایران به آستانه نوآوری رسیده‌است. همه اینها عواملی هستند که ضرورت پرداختن جدی به پایان‌نامه‌های دانشجویی را (که خود بخش قابل توجهی از تحقیقات دانشگاهی را شامل می‌شود) نشان می‌دهد. امید است سرمایه‌گذاری در علم و پژوهش (به معنی توجه به آینده کشور و توسعه پایدار و مطلوب) هرروز بیشتر و بهتر شود و پژوهش و فناوری به عنوان مفاهیم فراملی بیش

از پیش شناخته شوند. بنابراین باید امید داشت در برنامه‌ریزی‌های بومی کشور، تحولات جهانی در نظر گرفته شود و معیارهای بین‌المللی ملاک عمل قرار گیرد.

با درک ضرورت توسعه علم، بسط دانایی و تسهیل دسترسی جامعه به نتایج مطالعات پژوهشگران، سازمان انتشارات جهاددانشگاهی با برگزاری «جشنواره پایان‌نامه سال دانشجویی» اقدام به انتخاب بهترین پایان‌نامه‌ها در موضوعات مختلف دانشگاهی نموده‌است اثری که پیش روی شماست حاصل هشتمین دوره برگزاری جشنواره پایان‌نامه سال دانشجویی در سال ۸۳ می‌باشد که در قالب مجموعه پایان‌نامه‌های برگزیده هشتمین دوره پایان‌نامه سال دانشجویی منتشر می‌گردد.

با آرزوی توسعه و تعمیق این حرکت و با امید به جلب نظر تمامی اندیشمندان و دست‌اندرکاران عرصه پژوهش و نگارش از تمامی عزیزانی که سازمان انتشارات جهاددانشگاهی را در این راه همراهی کرده‌اند سپاسگزاری و تقدیر می‌نمائیم.

سازمان انتشارات جهاددانشگاهی
و دبیرخانه پایان نامه سال دانشجویی

فصل اول:
مقدمه

در دو دهۀ اخیر، تجارت الکترونیکی ـ انقلاب اینترنت، شبکه‌های کامپیوتری گسترده و فنّاوری اطلاعات در عرصۀ تجارت و بازرگانی- در بخش‌های خرده و عمده فروشی تحولات عمیقی را در روابط اقتصادی بین افراد، شرکت‌ها و دولت‌ها، و حرکت از مبادلات سنتی مبتنی بر کاغذ به سوی مبادلات الکترونیکی پدید آورده است. تجارت الکترونیکی، امروزه در شاخه‌های مختلفی از زندگی بشر وارد شده است، به گونه‌ای که خرید مایحتاج روزانه، امور بانکی، تحصیل و کار از راه دور، همگی به ساده‌ترین شکل ممکن با درنَوردیدن زمان و مکان در سراسر این کره خاکی به انجام می‌رسند. مدل‌های سیستم‌هایی که در حوزۀ تجارت الکترونیکی مطرح هستند، در یکی از پنج دستۀ کلی«بنگاه ـ بنگاه[۱]»، «بنگاه ـ مشتری[۲] ومشتری ـ بنگاه[۳]»، «مشتری- مشتری[٤]»، «بنگاه ـ دولت[٥] و دولت ـ بنگاه[٦]»، «مشتری ـ دولت[۷] و دولت ـ مشتری[۸] » قرار می‌گیرند[۹]. خرده‌فروشی (مثل amazon، ...) در ردۀ B۲C و C۲B قرار دارد. ردۀ C۲C (P۲P) شامل مواردی چون مزایده و مناقصه کالاها (مثل eBay) است. پرداخت عوارض و مالیات شرکت‌ها به سازمان‌های دولتی در ردۀ B۲G (B۲A) و G۲B (A۲B)، و جمع‌آوری کمک‌های مردمی و پرداخت مالیات بر درآمد از مثال‌های ردۀ C۲G (C۲A) و G۲C (A۲C) هستند (فرید و همکاران، ۱۳۸۰؛ نصیری‌مفخّم، اسفند ۱۳۸۰؛ نصیری‌مفخّم، ۱۳۸۲).

---

۱. Business to Business
۲. Business to Consumer (or Customer)
۳. Consumer to Business
٤. Consumer to Consumer or Person to Person
٥. Business to Administration or Business to Government
٦. Administration to Business or Government to Business
۷. Consumer to Administration or Consumer to Government
۸. Administration to Consumer or Government to Consumer
۹ـ مطابق معادل‌های فارسی مرکز ملی شماره‌گذاری کالا و خدمات ایران (وابسته به مؤسسه مطالعات و پژوهشهای بازرگانی) در فراخوان نخستین همایش بین‌المللی تجارت الکترونیکی و مالکیت فکری، بهمن ۸۰ .

سرعت، کارایی، کاهش هزینه‌ها و بهره‌برداری از فرصت‌های زودگذر، مزایایی است که استفاده از تجارت الکترونیکی را گریزناپذیر می‌سازد؛ ولی قبل از استفادهٔ گستردهٔ تجاری از اینترنت، بکارگیری روش‌های ایمن پرداخت حائز اهمیت هستند. ایدهٔ پرداخت الکترونیکی برای کالاها و خدمات روی اینترنت نیز، با افزایش تجاری شدن اینترنت و رشد تعداد کاربران و کاربردها، در دههٔ گذشته توسعه یافته است. همانگونه که در شکل ۱-۱ نیز مشاهده می‌شود، در یک فرایند کامل تجارت الکترونیکی که شامل بازاریابی، مذاکره، قرارداد و تنظیم توافق‌نامه، پرداخت، تحویل کالا و پشتیبانی است، سیستم‌های پرداخت نقش مهمی را به عنوان دروازه‌ای جهت ارتباط با بانک‌ها برای مبادلهٔ وجوه در مدل کلی هر چرخهٔ تجاری دارا هستند (نصیری‌مفخّم، ۱۳۸۲).

شکل ۱-۱- چرخهٔ تجارت الکترونیکی در حالت کلی

منبع: وید (۲۰۰۰)

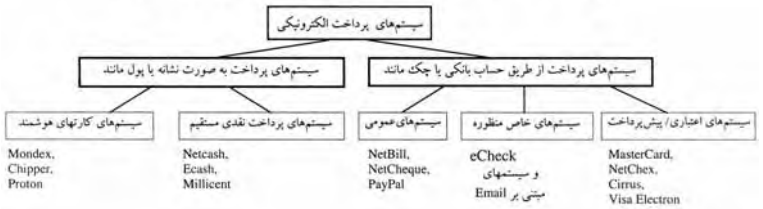
پرداخت الکترونیکی نقش بسیار حساس و کلیدی را ایفا می‌نماید و این امکان را به وجود می‌آورد که عمل پرداخت به سهولت، ارزان، سریع و با امنیت قابل قبولی در محیط اینترنت انجام گیرد.

در این فصل، ابتدا مروری گذرا بر سیستم‌های پرداخت الکترونیکی داریم و سپس نظر به اهمیت و حساسیت امنیت در سیستم‌های پرداخت الکترونیکی، به اختصار به این موضوع می‌پردازیم.

روش‌های پرداخت الکترونیکی

خریدار برای خرید در دنیای فیزیکی، مبلغ کالا را به صورت رو در رو توسط پول نقد، چک، کارت اعتباری، پیش‌پرداخت، و یا از طریق مراجعه به بانک به وسیله حوالهٔ بانکی، به فروشنده پرداخت می‌کند. در چندین سال گذشته، سیستم‌هایی برای پرداخت الکترونیکی به روشهای اعتباری، چک و پول نقد در مؤسسات تحقیقاتی و کمیته‌های استاندارد معرفی شده است. برای

شکل ۱-۲- طبقه‌بندی سیستمهای پرداخت الکترونیکی از نظر نحوهٔ انتقال



منبع: ابراژویچ، ۲۰۰۱

خرید در دنیای مجازی نیز، از معادل‌های همین روش‌ها برای پرداخت روی اینترنت استفاده می‌شوند

(چان و همکاران، ۲۰۰۱؛ سازمان ملل، ۲۰۰۱؛ نصیری‌مفخّم، ۱۳۸۲).
در روش اعتباری (مثلاً کارت‌های اعتباری) مبلغ پرداختی توسط یک مرکز اعتباری، پرداخت و سپس آن مبلغ از اعتبار کاربر کم شده و در زمان خاصی، مبلغ واقعی توسط کاربر (یا از حساب بانکی وی) به آن مرکز پرداخت می‌گردد. در روش چک، مبلغ پرداختی توسط یک مدرک معتبر برای فروشنده ارسال می‌شود و سپس این مدرک همانند چک فیزیکی از طریق حساب بانکی خریدار نقد می‌گردد. در روش پول نقد، کاربر به ازای پرداخت مبلغی، پول الکترونیکی دریافت می‌کند و در موقع خرید برای فروشنده ارسال می‌دارد. این روش‌ها از نظر نحوهٔ انتقال پول همانگونه که در شکل ۱-۲ نشان داده است، به دو نوع پرداخت از طریق حساب بانکی[۱] (تحریری[۲] یا چک‌مانند[۳]) و پرداخت بصورت نشانه‌ای[۱]

---

۱ **Account-Based**
۲ **notational**
۳ **check-like**

(پول‌مانند[۲]) تقسیم می‌شوند[۳] (ابراژویچ، ۲۰۰۱-۱؛ اسوکان و همکاران، ۱۹۹۹؛ وبر، ۱۹۹۸؛ یو و همکاران، ۲۰۰۲؛ فانی، ۱۳۸۰، نصیری‌مفخّم، ۱۳۸۲، بخش ۲-۳-۱).

در سیستم‌های پرداخت از طریق حساب بانکی، هویت پرداخت‌کننده مخفی نیست. کاربران با انتقال پیام پرداخت، مبلغ پرداخت و سفارش‌های پرداخت را می‌دهند. این روش پرداخت به صورت‌های اعتباری[٤] و یا پیش‌پرداخت[٥] انجام می‌شود. در مدل پیش‌پرداخت، مشتری باید در حسابش وجه کافی داشته باشد و موقع انجام تراکنش، از حساب او کسر می‌شود. در مدل اعتباری، مطالبات به حساب مشتری ارسال می‌شود و او بعداً صورتحساب را می‌پردازد. در سیستم‌های پرداخت بصورت نشانه‌ای (یا پول مانند) ، مشتری ژتونها یا نشانه‌هایی از شرکت صادرکننده، خریداری کرده و با ذخیره نمودن در کارت هوشمند یا روی دیسک کامپیوتر، از آنها برای پرداخت استفاده می‌کند. نشانه‌ها نمایانگر سکه‌ها یا اسکناس‌ها هستند[٦].

استفاده‌کنندگان از ابزارهای سنتی پرداخت از مشکلات متعدد امنیتی شناخته شده رنج می‌برند. مثلاً: پول می‌تواند جعل شود، امضاها می‌تواند تقلید شود، و چک‌ها می‌تواند برگشت بخورد. ابزارهای الکترونیکی پرداخت نیز همان معایب را دارا هستند، و علاوه بر آن برخی مخاطرات دیگر را هم در بردارند. به طور نمونه: برخلاف کاغذ، اسناد دیجیتالی اغلب می‌توانند توسط اشخاص به طور کامل کپی شوند؛ امضاهای دیجیتالی[۷] می‌تواند توسط هر کسی که کلید امضای محرمانهٔ رمزنگاری را بداند تولید شود؛ نام خریدار می‌تواند با هر پرداختی نظیر شود، ضمن اینکه اختفای پول نقد نیز در میان نیست. ولی

---

۱ **Token-Based**

۲. **cash-like**

٦ـ البته به دلیل ماهیت چک که در حکم پول است ولی واقعاً یک نوشته است، در برخی تحقیقات، چک را از نوع ترکیبی بیان می‌کنند.

٤. **Credit**

٥. **Debit**

۹ ـ چهار روش پرداخت الکترونیکی (پول الکترونیکی، چک الکترونیکی، کارت اعتباری روی اینترنت، و حواله الکترونیکی) به ترتیب بر اساس مدل‌های "پول‌مانند - مستقیم"، "مبتنی بر حساب - مستقیم"، "مبتنی بر حساب - غیر مستقیم - دادنی" و "مبتنی بر حساب - غیر مستقیم - گرفتنی" هستند (اسوکان، ۱۹۹۹؛ وبر، ۱۹۹۸؛ حاجبی، ۱۳۸۱؛ نصیری‌مفخّم، ۱۳۸۲، بخش ۲-۳-۲).

۱ـ بخش ۱ـ۲ را ببینید.

چنانچه سیستم‌های پرداخت الکترونیکی به دقت طراحی شوند، می‌توانند امنیت بیشتری نسبت به ابزارهای سنتی پرداخت، همراه با انعطاف‌پذیری و راحتی استفاده، فراهم آورند (اسوکان و همکاران، ۱۹۹۹؛ سیربو، ۱۹۹۷). ابزارهای امنیتی جهت تعیین هویت فرستنده، تمامیت و محرمانگی اطلاعات، جلوگیری از افشای محتوای پیام و یا ارسال پیام توسط فرد غیر مجاز، و عدم انکار توسط فرستنده و گیرنده، مورد نیاز می‌باشد.

سیستم‌های پرداخت که بر اساس ارائه امن کارت اعتباری روی اینترنت هستند[۱]، از زیرساختارهای موجود کارت اعتباری، همچون SET[۲]، استفاده غیر مستقیم می‌کنند. مؤلفه‌های دخیل در پرداخت با کارت اعتباری، تاجر (فروشنده)، دارندهٔ کارت (خریدار)، صادرکننده (بانک صادرکنندهٔ کارت اعتباری)، پذیرنده (بانک کارگزار تاجر برای اتصال به صادرکنندگان چندگانه)، دروازهٔ پرداخت (متصل به پذیرنده، بین سیستم SET و شبکهٔ مالی سیستم کارت اعتباری فعلی) و مراجع گواهی هستند. پروتکل SET بین خریدار و فروشنده، و بین فروشنده و دروازهٔ پرداخت است (برینوف، ۲۰۰۱؛ چان و همکاران، ۲۰۰۱؛ ست، ۲۰۰۵؛ شریف، ۲۰۰۰؛ نصیری‌مفخّم، ۱۳۸۲).

شماره کارت اعتباری مشتری با استفاده از رمزنگاری کلید عمومی، به گونه‌ای رمزنگاری می‌شود که فقط توسط بازرگان یا طرف سوم معامله یعنی سرویس پردازش پرداخت قابل خواندن است. بزرگترین مزیت این روش آن است که مشتری نیازی به ثبت‌نام‌شدن توسط سرویس پرداخت شبکه‌ای ندارد. اما بدون ثبت نام مشتریان، معاملات کارت اعتباری رمزنگاری شده، شامل امضا نمی‌باشد. هر کسی با دانستن شماره کارت اعتباری مشتری می‌تواند سفارش پرداخت را صادر کند، همانطور که می‌تواند یک سفارش تقلبی روی تلفن بدهد. همچنین از آنجایی که پرداختهای پردازش شده با این روش به صورت هزینه‌های کارت اعتباری استاندارد پردازش می‌شود، مخارج آن قدر زیاد است که این روش برای پرداختهای خرد مناسب نیست (سیربو، ۱۹۹۷؛ حاجبی، ۱۳۸۱؛ نصیری‌مفخّم، ۱۳۸۲).

---

۲ ـ SET، InstaBuy، SSL، و VCC، عمومی و پیشرفته‌ترین سیستم‌های پرداخت ارتباط پیوسته (روی اینترنت) با کارت اعتباری هستند (وایز، ۲۰۰۱؛ نصیری‌مفخّم، ۱۳۸۲). برای اطلاعات بیشتر به (نصیری‌مفخّم، ۱۳۸۲، بخش ۲-۳-٤-۲) مراجعه شود.

۲. Secure Electronic Transaction

سیستم‌های پول الکترونیکی به دو صورت نرم‌افزاری و مبتنی بر کارت هستند[۱]. Mondex یکی از سیستم‌های معروف پول الکترونیکی مبتنی بر کارت است که خدمات با ارتباط ناپیوسته را نیز برای مبادله وجه ارائه می‌دهد. (ابراژویچ، ۲۰۰۱؛ چان و همکاران، ۲۰۰۱؛ سازمان ملل، ۲۰۰۱؛ وبر، ۱۹۹۸؛ نصیری‌مفخّم، ۱۳۸۲) Mondex برای پرداخت‌های شخص به شخص مثل پرداخت‌های اینترنتی، پرداخت‌های کوچک، ذخیره اطلاعات شخصی و نیز به عنوان کارت تلفن با سطح سرویس‌دهی خیلی بالا، قابلیت دارد. هر کارت Mondex یک شماره ID یکتا دارد، که این شماره هنگام صدور کارت در بانک به شخص داده می‌شود. عیب این گونه کارتها آن است که نیاز به زیر ساختار حمایتی دارد، زیرا در صورت سرقت شدن، در واقع پول درون آن گم شده است (چان و همکاران، ۲۰۰۱؛ نصیری‌مفخّم، ۱۳۸۲).

در میان ابزارهای پرداخت الکترونیکی، پول الکترونیکی با ایجاد نوع کاملاً جدیدی از پول و سوءاستفادهٔ پول‌شویان از اختفای آن، به سیستم مالی آسیب رسانده و به دلیل مکانیزم‌های امنیتی ساده‌ای که دارد، برای پرداخت‌های کلان بازرگانی مناسب نیست. همچنین، کارت‌های اعتباری علاوه بر محدودیت مبلغ پرداخت، از جهت احراز هویت ضعیف، امکان انکار از جانب یکی از طرفین، امکان تقلب ساده، و هزینه بالای تراکنش‌ها آسیب پذیرند. فروشندگان کالاها باید هزینهٔ سنگین پردازش اطلاعات کارت اعتباری مشتریان را متحمل شوند، به ویژه آن که تاجران خرد به دلیل قوانین مربوطه، قادر به دریافت کارت اعتباری نیستند (دانی و همکاران، ۲۰۰۱؛ چاوم و همکاران، ۱۹۹۷؛ سیربو، ۱۹۹۷؛ شریف، ۲۰۰۰؛ کمیته تحقیقاتی گروه کاربران ایرانی سویفت، ۱۳۸۲؛ نصیری‌مفخّم، ۱۳۸۲).

برای تجارت B۲B که مبلغ انتقالی معمولاً بزرگ است، روش‌های چک و پرداخت بستانکار/بدهکار مناسب هستند. از طرفی هیچکدام از ابزارهای پرداخت الکترونیکی اعتباری و نقدی، مزایای چک کاغذی را دارا نیستند و روش‌های بدهکاری و بستانکاری الکترونیکی، الزامی قانونی برای پرداخت ایجاد نمی‌کنند. بنابراین به یک سیستم پرداخت الکترونیکی جدید نیاز داریم

---

۱ ـ Visa Cash، Mondex، و Ecash از عمومی و پیشرفته‌ترین سیستم‌های پول الکترونیکی بوده(وایز، ۲۰۰۱؛ نصیری‌مفخّم، ۱۳۸۲) و Proton، Visa Cash، و Mondex از مثال‌های "پول‌کارت‌های هوشمند هستند.

که شامل مزایا و جایگاه قانونی چک‌های کاغذی بوده و معایب دستی بودن پرداخت مبتنی بر کاغذ را نداشته باشد (اندرسون، ۱۹۹۸؛ ای‌چک‌ورلدواید، f ۲۰۰۱؛ شریف، ۲۰۰۰؛ نصیری‌مفخّم، ۱۳۸۲).

چک الکترونیکی، نسخهٔ الکترونیکی چک کاغذی، رایج‌ترین ابزار پرداخت غیرنقدی است. در فصل دوم، ضمن آشنایی با فرایند پرداخت چک و چک الکترونیکی، به بررسی و مقایسهٔ چک الکترونیکی با سایر روش‌های پرداخت الکترونیکی پرداخته و تحقیقات صورت گرفته در جهان دربارهٔ سیستم‌های چک الکترونیکی را مرور می‌کنیم.

از آنجا که ذات سیستم‌های تجارت الکترونیکی به گونه‌ای است که فرصت‌های بیشتری برای تخلفات امنیتی در اختیار قرار می‌دهند و نیازمند سطوح بالایی از کنترل امنیتی، چه از لحاظ تکنولوژی و چه از لحاظ عملکرد می‌باشد، و از طرفی نظر به اینکه تحقق و پیاده‌سازی سیستم‌های پرداخت الکترونیکی در سیستم‌های مالی، بدون لحاظ نمودن امنیت مطابق با استانداردهای جهانی، امکان پذیر نخواهد بود، لذا در ادامهٔ این فصل به موضوع امنیت در سیستم‌های پرداخت الکترونیکی می‌پردازیم.

امنیت در سیستم‌های پرداخت الکترونیکی

ویژگی‌هایی که در تحقیقات انجام شده برای سیستم‌های پرداخت الکترونیکی به آنها اشاره گردیده است، عبارتند از: ایمنی و امنیت[۱]، قابلیت اطمینان[۲]، قابلیت ارتقا، مقیاس‌پذیری و قابلیت تغییر اندازه[۳]، ناشناخته بودن و اختفا[٤]، پذیرش، تطابق و تقبل[٥]، مشتری‌مداری، انعطاف پذیری[٦]، قابلیت تبدیل[۷]، بازدهی و کارآیی[۸]، آسانی تجمیع و همراهی با برنامه‌های کاربردی، استفاده آسان و سادگی کار[۹]، نوع مجوز[۱]، قابلیت انتقال[۲]، کاربست‌پذیری[۳]،

---

۱. security
۲. reliability
۳. scalability
٤. anonymity
٥. acceptability
٦. flexibility
۷. convertibility
۸. efficiency
۹. ease of use or usability

قابلیت ردگیری[٤]، اعتماد[٥]، بلادرنگ نبودن[٦]، باز بودن سیستم[٧] و سازگاری[٨]، و همانگونه که در فصل پنجم آمده است، می‌توان این ویژگی‌ها را در گروه کوچکتری دسته‌بندی کرد[٩]. نیازمندیهای اولیه امنیتی در همه سیستم‌های پرداخت، معمولاً شامل هویت‌شناسی[١٠]، جامعیت[١١]، مجازشناسی[١٢]، محرمانگی[١٣]، قابلیت دسترسی و قابلیت اطمینان[١٤] است. تکنیک‌های رمزنگاری[١٥]، ابزارهای اساسی در امن‌کردن مبادلات الکترونیکی و پروتکل‌های پرداخت روی شبکه‌های باز و نا امن هستند که جهت تأمین و بررسی جامعیت، محرمانگی، هویت‌شناسی، نفی انکار و غیره به کار می‌آیند. رمزنگاری متقارن[١٦] (رمزنگاری کلید سری[١٧]) و رمزنگاری نامتقارن[١٨] (رمزنگاری کلید عمومی[١٩])، دو نوع از رمزنگاری‌های معروف هستند. از جمله مهم‌ترین کاربردهای رمزنگاری نامتقارن، در امضای دیجیتالی است (ابراژویچ، ۲۰۰۱؛ اسوکان وهمکاران، ۱۹۹۹؛ چان و همکاران، ۲۰۰۱؛ کلیسنز و همکاران، ۲۰۰۱؛ فریرا، ۱۹۹۸؛ گریگ، ۲۰۰۰؛ هوانگ و همکاران، ۲۰۰۱؛ کلی، ۱۹۹۷؛ نیومن و همکاران، ۱۹۹۵؛ اشنیر، ۱۹۹٤؛ شریف، ۲۰۰۰؛ سیربو، ۱۹۹۷؛ وید،

---

۱. authorization type
۲. transferability
۳. applicability
٤. traceability
٥. trust
٦. offline
۷. openness
۸. interoperability

۱۳ ـ برای تعاریف این ویژگی‌ها به (نصیری‌مفخّم، ۱۳۸۲، فصل دوم، بخش ۲-۳-۳، صص.۲۰-۱۷ و فصل هفتم، بخش ۷-۲، صص. ١٦٤-١٦٢) مراجعه کنید.

۱۰. Authentication
۱۱. integrity
۱۲. Authorization
۱۳. confidentiality
١٤. reliability
١٥. encryption
١٦. Symmetric
۱۷. Secret key
۱۸. Asymmetric
۱۹. Public key

۲۰۰۰، وبر، ۱۹۹۸؛ یو و همکاران؛ ۲۰۰۲؛ حاجبی، ۱۳۸۱؛ فانی، ۱۳۸۰، نصیری‌مفخّم، ۱۳۸۲).

امضای دیجیتالی و زیرساختار رمز نامتقارن (بستر کلید عمومی ـ PKI)[۱]

امضای دیجیتالی؛ احراز هویت، نفی انکار، محرمانگی و جامعیت داده را تأمین می‌کند. امضای دیجیتالی، رمزگذاری پیام با کلید خصوصی فرستنده است[۲]. در واقع، رمزگذاری روی خلاصه‌ای از پیام که توسط یک الگوریتم درهم‌سازی[۳] تولید می‌شود، صورت می‌گیرد. فرض کنیم گیرنده B، خواهان دریافت پیامی از فرستنده A، روی مسیر ناامن اطلاعاتی است. ابتدا B و A کلیدهای عمومی خود را به یکدیگر می‌فرستند (کلید عمومی نیازی به اختفا ندارد و هر کسی می‌تواند کلید عمومی دیگران را داشته باشد). برای آنکه B مطمئن باشد که پیام از طرف شخص A آمده و در بین راه توسط پیام شخص دیگری جایگزین نشده است، A، پیام ارسالی را امضا می‌کند. یک خلاصه پیام[٤]، از پیام تولید کرده و آنرا با کلید خصوصی خود ـ که منحصراً نزد خود او است ـ رمز می‌کند. سپس، این خلاصه پیام را به خود پیام اضافه کرده و برای B ارسال می‌کند. این پیام فقط با کلید عمومی A به صورت موفقیت‌آمیز قابل رمزگشایی است. B، خلاصه پیام رمزشده را از اصل پیام جدا کرده و آن را با کلید عمومی A رمزگشایی می‌کند. سپس، این خلاصه بدست آمده را با خلاصه اصل پیام که خود آنرا تولید می‌کند مقایسه کرده، و چنانچه مطابقت داشته باشد، بدین معنی است که فرستنده، همان کسی بوده که ادعا کرده است (A و نه شخص دیگری)؛ چون کلید خصوصی متناظر کلید عمومی وی فقط نزد خود اوست، لذا *احراز هویت* می‌شود. همچنین در صورت تطابق نتیجه، *جامعیت* داده نیز برقرار است. پس پیام دست نخورده باقی مانده است؛ چرا که در غیر این صورت نتایج با هم مطابقت نخواهد داشت. از طرف دیگر، همین که صحت امضا احراز شد، A نمی‌تواند فرستادن پیام را انکار کند؛ چرا که

---

۱. Publik Key Infrastructure

۳ ـ RSA و DSS از الگوریتمهای مورد استفاده در امضاهای دیجیتالی هستند. برای آشنایی بیشتر با امضاهای دیجیتالی به (چان و همکاران، ۲۰۰۱؛ گالبریث، ۲۰۰۲؛ گِرُدکِل، ۱۹۹۹؛ شِریف، ۲۰۰۰؛ وایلز، ۲۰۰۱؛ نصیری‌مفخّم، ۱۳۸۲، بخش ۲-٤-۲) مراجعه شود.

۳. hash

٤. Message digest

کلید خصوصی او فقط در اختیار شخص او و نه فرد دیگری است، و B می‌فهمد که پیام از طرف شخص A ارسال شده است و بدین طریق *نفی انکار ارسال* از جانب A می‌شود. برای حفظ *محرمانگی* و اطمینان از اینکه فرد دیگری غیر از گیرنده مورد نظر (B)، نتواند پیام را بخواند و همچنین B نتواند دریافت پیام را انکار کند، کافی است که A، پیام امضا شده را با کلید عمومی B، رمز کرده و سپس ارسال کند. B، باید به ترتیب عکس A عمل کرده، و ابتدا پیام را با کلید خصوصی خود رمزگشایی کند و سپس مراحل یاد شده را پی بگیرد. این پیام فقط و فقط با کلید خصوصی B که منحصراً نزد B است، می‌تواند رمزگشایی شود و محرمانه بماند، به طوری که دیگران قادر به مشاهدهٔ اصل پیام نباشند. (نصیری‌مفخّم، ۱۳۸۲).

امضاهای دیجیتالی، سندیتی بر هویت افراد نیستند. A و B برای آنکه مطمئن باشند که کلیدهای عمومی درستی از یکدیگر در اختیار دارند و شخص دیگری در میان راه، کلید عمومی خود را تحویل نداده است، تأییدیه‌ای[۱] از یک سازمان ثالث مورد اعتماد[۲] ارایه می‌کنند. این گواهی، تضمین می‌کند که کلید عمومی متعلق به شخص خاصی است که آن سازمان هویت او را قبل از ضمانت، احراز کرده است[۳]. طرفین یک تراکنش جهت اخذ تأییدهای لازم، باید در مسیر گواهی به یک مسئول گواهی مشترک مراجعه کنند. از نزدیک‌ترین مسئول گواهی خواسته می‌شود که کلید عمومی مربوط به گواهی مهرشده با امضای دیجیتالی مسئول را بفرستد. درخواست در زنجیرهٔ مسئولان یا مسیر گواهی بالا می‌رود تا به بالای هرم گواهی یعنی به مسئول ریشه (RA[۴]) برسد (وایز، ۲۰۰۱؛ پوررستم، ۱۳۸۱؛ عباسی، ۱۳۸۱؛ نصیری‌مفخّم، ۱۳۸۲).

---

۱ ــ مدلهای اعتماد در PKI بر اساس استاندارد ISO X.۵۰۹V۳ یا PGP هستند (کریپتوماتیک، ۲۰۰۳؛ گالبریث، ۲۰۰۲؛ اشنیر، ۱۹۹٤؛ شیموس، ۲۰۰۲؛ شریف، ۲۰۰۰؛ تاننباوم، ؛ سازمان ملل، ۲۰۰۱؛ وایز، ۲۰۰۱؛ بختیاری، ۱۳۸۱؛ پوررستم، ۱۳۸۱؛ نصیری‌مفخّم، ۱۳۸۲).

۲. Certificate Authority

۳ ـ برخی از متداول‌ترین CAها عبارتند از:

(VeriSign, Inc.) www.verisign.com ،(Thawte Consulting) www.thawte.com ،(GTE CyberTrust)www.get.com/cybertrust،(BelSignNV/SA) www.belsign.com ABAecom www.abaecom.com ،(Equifax Secure CA) www.equifaxsecure.com و E-Cetify Corporation) www.e-certify.com

٤. Root Authority

فصل دوم:
چک الکترونیکی

چک کاغذی، رایج‌ترین ابزار پرداخت غیرنقدی است، بطوریکه هیچکدام از ابزارهای پرداخت الکترونیکی اعتباری و نقدی، مزایای چک کاغذی را دارا نبوده و برای پرداختهای کلان بازرگانی مناسب نیستند. یک چک کاغذی، یک سند کاغذی امضا شده است که به بانک شخص امضا کننده دستور می‌دهد مبلغ معینی پول را از حساب امضاکننده، بعد از تاریخ مشخصی بپردازد. چک‌های کاغذی، مستقیماً از پرداخت‌کننده به دریافت‌کننده داده می‌شود، به طوری که زمان و هدف پرداخت کاملاً واضح است. مزیت چک‌های کاغذی این است که هر کدام از پرداخت‌کنندگان و دریافت‌کنندگان می‌توانند اشخاص، بازرگانانِ خرد، واسطه‌ها، شرکت‌ها، دولت‌ها یا هر نوع سازمانی باشند. با وجود نقَش مهم و منحصر بفردی که چک‌های کاغذی، در تجارت دارند، اما به دلیل آنکه در هنگام نوشتن آنها، هیچ مجازشناسی صورت نمی‌گیرد، مشکلات آنها به عنوان مکانیزم‌های پرداخت، روز به روز در حال افزایش است[1]. بنابراین به یک سیستم پرداخت الکترونیکی جدید نیاز داریم که شامل مزایا و جایگاه قانونی چک‌های کاغذی بوده و معایب دستی بودن پرداخت مبتنی بر کاغذ را نداشته باشد (ای‌چک، ۲۰۰۵؛ ای‌چک‌ورلدواید، ۲۰۰۵؛ ای‌چک‌ورلدواید، ۲۰۰۱؛ شریف، ۲۰۰۰؛ نصیری‌مفخّم، ۱۳۸۲؛ نصیری‌مفخّم و همکاران، ۱۳۸۳).

امروزه محصولاتی تحت عنوان چک الکترونیکی[2]، تهیه شده‌اند که همگی یک چک الکترونیکی به معنای واقعی کلمه نیستند. این محصولات در یکی از

۱ـ در ایالات متحده تقریباً ۷۰ میلیون چک توسط تجار، مشتریان و مؤسسات دولتی نوشته می‌شود (گرانت، ۲۰۰۰ ؛ نصیری‌مفخّم، ۱۳۸۲) که هزینه آنها حدود ۱٪ تولید ناخالص داخلی است. ضرر ناشی از تقلب در چک سالانه بالغ بـر ۵۳ میلـیارد دلار بـرآورد مـی‌شـود که برای بانک‌هایی که به نامشان نوشته می‌شود ۱/۳٤ میلیارد دلار و برای خرده‌فروشان و دیگر دریافت‌کنندگان، ۵۲ میلیارد دلار است.

۲ . eCheck

دسته‌های «الکترونیکی کردن چک[۱]»، «تصویر نمودن چک[۲]»، «تبدیل چک[۳]»، «جایگزینی چک[٤]»، و «نوشته‌جات امضا نشده[٥]» واقع می‌شوند (شریف، ۲۰۰۰؛ نصیری‌مفخّم، ۱۳۸۲). ولی چک الکترونیکی، یک چک تمام الکترونیکی، و یک جایگزین الکترونیکی برای چک کاغذی است. چک‌های الکترونیکی همچون چک‌های کاغذی، دارای الزام تعهدآور قانونی برای پرداخت هستند در آن و به جای امضاهای دست‌نوشته، از امضاهای دیجیتالی در آن استفاده می‌شود. چک الکترونیکی، یک سند دیجیتالی امضا شده به صورت الکترونیکی است که می‌تواند سایر اسناد و اطلاعات صورتحساب، اعلامیه‌ها، پشت‌نویسی و واگذاری را نیز با خود همراه داشته باشد.

مزیت دیگر چک الکترونیکی، این است که روی استانداردها و شبکه‌های باز طراحی می‌شود و هر چند مانند سایر روش‌های پرداخت الکترونیکی می‌تواند در معرض حملات واقع شود، ولی برخلاف دیگر روش‌های پرداخت، از یک طرف با بهره‌گیری از مطمئن‌ترین روش‌ها، هویت‌شناسی، مجازشناسی، محرمانگی، جامعیت، نفی‌انکار و جلوگیری از دوبار خرج‌شدگی را تأمین می‌کند، و از طرف دیگر با اتکا به قانون چک، از الزام قانونی پرداخت‌شدن برخوردار است که استفاده از آن را همچون نسخهٔ کاغذی خود، مطمئن و پرطرفدار می‌سازد. وقتی سایر روش‌های پرداخت، اینترنتی می‌شوند، قطعیت پرداخت‌شدن آنها بدلیل مشکلات امنیتی شبکه‌های باز، کمتر می‌شود. در مورد چک کاغذی، با وجود الزام قانونی پرداخت از طرف صادرکننده، به دلیل مشکلاتی همچون موجود نبودن وجه کافی، قطعیت پرداخت‌شدن آن نامعلوم و نسبت به سایر روش‌های سنتی کمتر است. ولی با الکترونیکی‌شدن خود چک و مجازشناسی بلادرنگ آن با بهره‌گیری از امضاها و گواهی‌های

---

۱. **Check electronification**
۲. **Check imaging**
۳. **Check conversion**
٤. **Check replacement**
٥. **Unsigned drafts**

دیجیتالی، و امکان بررسی وجود وجه کافی در حساب شخص صادرکننده، قطعیت پرداخت‌شدن آن معلوم و تضمین می‌شود، بدون آنکه (همچون کارت‌های اعتباری) ضرری متوجه مؤسسهٔ اعتباری حامی یا دریافت‌کنندهٔ چک باشد و بدین طریق نسبت به نسخهٔ فیزیکی خود، در جایگاه بالاتری قرار می‌گیرد. دیگر آنکه، چون چک الکترونیکی از همان جریان پرداخت و پایاپای چک کاغذی پیروی می‌کند، بانک‌ها با سرمایه‌گذاری کمی می‌توانند این فنّاوری جدید را عرضه کنند، مضافاً آنکه سیستم چک الکترونیکی می‌تواند با تجمیع با سیستم‌های پایاپای مکانیزهٔ بانکی، ضمن برخورداری از هزینهٔ کمتر پردازش، بر سهولت، صحت و سرعت تسویهٔ حساب‌های بانکی بیفزاید. پس برای بانک‌ها هزینهٔ حمل چک‌ها و تحویل و پست صورت‌حساب‌ها حذف شده و با دسترسی سریع به داده‌ها، مدیریت نقدینگی بهبود یافته و در ارایهٔ خدمات به مشتری مؤثر است. لذا بانکها از اینکه نقش خود را در تراکنشهای مالی حفظ خواهند کرد، علاقمند به چک الکترونیکی خواهند بود. تاجران نیز، به دلیل صرفه‌جوئی در هزینه‌ها و زمان پردازش تراکنش‌ها و تهیه گزارش‌های مدیریتی بر اساس داده‌های تراکنش‌ها، و کاهش برگشت چک‌های واگذاری، به چک الکترونیکی علاقمند خواهند بود. همچنان‌که بخش B۲B گسترش می‌یابد، سیستم چک‌های الکترونیکی مهم‌تر می‌شود (دانی و همکار، ۲۰۰۱؛ ای‌چک، ۲۰۰۵؛ ای‌چک‌ورلدواید، ۲۰۰۵؛ ای‌چک‌ورلدواید، ۲۰۰۱؛ جفی، ۱۹۹۸؛ سیربو، ۱۹۹۷؛ وید، ۱۹۹۹؛ نصیری‌مفخّم، ۱۳۸۲؛ نصیری‌مفخّم و همکاران، دی ۱۳۸۲ و ۱۳۸۳).

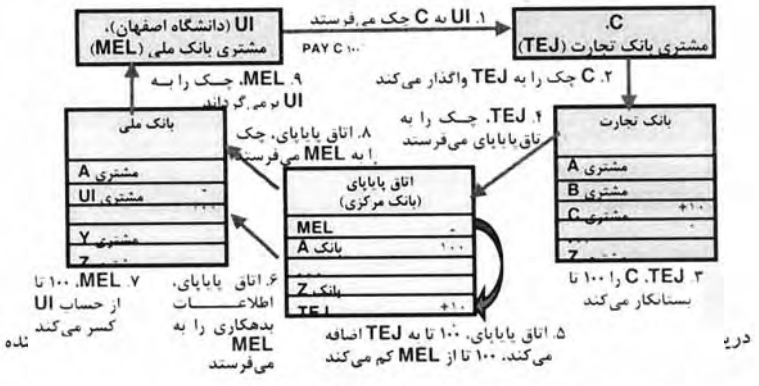
فرآیند پرداخت چک کاغذی

در مدل چک کاغذی، ارتباط مستقیم بین پرداخت‌کننده و دریافت‌کننده وجود دارد. پرداخت‌کننده، یک سند پرداخت به دریافت‌کننده می‌دهد. دریافت‌کننده، این سند را در بانک کارگزار خود به حساب خود می‌گذارد. سپس بانک کارگزار دریافت‌کننده و بانک کارگزار پرداخت‌کننده با هم پایاپای و تسویه می‌کنند. شکل ۲-۱، نشان‌دهندهٔ این مدل است (اسوکان و مکاران،

۱۹۹۹؛ برینوف، ۲۰۰۱؛ سیربو، ۱۹۹۷؛ وبر، ۱۹۹۸؛ حاجبی، ۱۳۸۱؛ نصیری‌مفخّم، ۱۳۸۲).

در یک فرایند پرداخت از خریدار تا فروشنده از طریق بانک، مؤلفه‌های بسیاری دخالت دارند که در شکل ۲-۲ مشاهده می‌کنیم.

شکل ۲-۳- روند پایاپای چکهای مشتریان در دو بانک مجزا



منبع: شیموس (۲۰۰۲) و نصیری‌مفخّم (۱۳۸۲)

شکل ۲-۲- فرایند پرداخت

منبع: شیموس (۲۰۰۲)

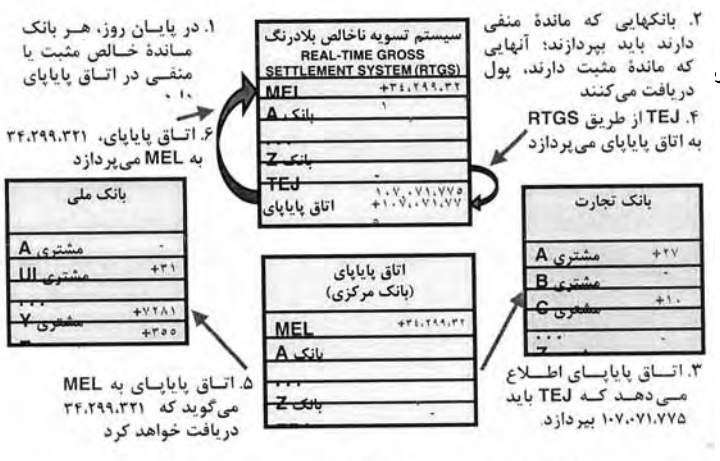
وقتی حساب‌های پرداخت‌کننده و دریافت‌کننده در بانک‌های متفاوت باشد، چک باید از میان یک سیستم پایاپای و تسویه مرکزی پردازش شود. در این حالت، با ارسال دستور پرداخت (حمل چک‌ها به اتاق پایاپای) و مبادلهٔ چک‌ها، پس از انجام عملیات حسابداری و تنظیم سندها، با بدهکار و بستانکار شدن خالص هر بانک، عملیات پایاپای[1] چک‌ها پایان می‌پذیرد. روند پایاپای چک‌ها، در شکل ۲-۳ آمده است (نصیری‌مفخّم، ۱۳۸۲).

اما زمانی‌که ارزش و پول واقعی جابجا شود و مستقیم یا با واسطه (بانک مرکزی) به بانک طرف مقابل رسانده شود، تسویه[2] نیز صورت گرفته است. شکل ۲-٤، نحوهٔ تسویه[3] حساب‌های مربوطه را در دو بانک مجزا نشان می‌دهد (نصیری‌مفخّم، ۱۳۸۲).

۲-۲ سناریوهای پردازش چک الکترونیکی

کنسرسیوم فناوری خدمات مالی (FSTC)[3] چهار سناریو برای پردازش چک‌های الکترونیکی بیان می‌کند که در شکل ۲-۵ نشان داده شده است. چک الکترونیکی به صورت سندی دیجیتالی (مثلاً با قالب XML) است که توسط پرداخت‌کننده، نوشته و امضای دیجیتالی می‌شود و برای دریافت‌کننده ارسال می‌گردد. دریافت‌کننده نیز آن را با امضای دیجیتالی خود پشت‌نویسی کرده و به بانک خود واگذار می‌کند تا با بانک پرداخت‌کننده از طریق سیستم پایاپای موجود تسویه نماید. هریک از کاربران و بانک‌ها گواهی‌هایی دیجیتالی برای اثبات صحت امضای خود دارند. بانک، امضای دیجیتالی روی چک را با کلید عمومی پرداخت‌کننده بررسی می‌کند. کلید عمومیِ پرداخت‌کننده همراه با گواهی دیجیتالی پرداخت‌کننده به بانک ارسال می‌شود (اندرسون، ۱۹۹۸؛ چان و همکاران، ۲۰۰۱؛ دانی و همکاران، ۲۰۰۱؛ شریف، ۲۰۰۰؛ نصیری‌مفخّم، ۱۳۸۲).

شکل ۲-٤- روند تسویه چک‌های مشتریان در دو بانک مجزا



منبع: شیموس (۲۰۰۲) و نصیری‌مفخّم (۱۳۸۲)

حالت (الف)، همان سناریویی است که در فوق توضیح داده شد. از حالت (ب) وقتی استفاده می‌شود که بانک دریافت‌کننده، چک الکترونیکی را حمایت نمی‌کند و دریافت‌کننده، چک را مستقیم به بانک پرداخت‌کننده می‌فرستد. در حالت (ج)، دریافت‌کننده، یک حساب خاص معروف به صندوق پرداخت[۱] در بانکش باز می‌کند و بانک با این حساب، چک‌های الکترونیکی دریافت‌کننده را می‌پذیرد. این روش برای مراکز بزرگ که تعداد زیادی چک را باید بررسی کنند، مفید است. بعد از دریافت چک الکترونیکی توسط بانک، بقیه مراحل مثل حالت (الف) است. حالت (د) اساساً، همان روش پرداخت بستانکار/ بدهکار است. ابتدا پرداخت‌کننده، چک الکترونیکی را به بانک خود می‌فرستد. سپس بانک از طریق سیستم موجود انتقال وجوه الکترونیکی، حساب دریافت‌کننده را بستانکار می‌کند. ارسال و دریافت چک‌های الکترونیکی نیز فقط مستلزم سه عنصر ساده است. اول باید قابلیت ارسال و دریافت نامه الکترونیکی را داشت. دوم باید از سخت‌افزار امنیتی لازم همچون کارت تراشه‌ای یا دستگاه خوانندهٔ کارت PCMCIA (که بزودی ابزار استانداردی روی همهٔ کامپیوترها می‌شود) (شیموس، ۲۰۰۲) بهره‌مند بود. سوم ، باید در بانکی که دسته چک‌ها و خدمات الکترونیکی عرضه می‌دارد، حساب بانکی داشت. (اندرسون، ۱۹۹۸ ؛ چان و همکاران، ۲۰۰۱؛ گلیناس، ۲۰۰۱؛ نصیری‌مفخّم، ۱۳۸۲).

۲-۳ تحقیقات انجام شده در مورد سیستم‌های چک الکترونیکی

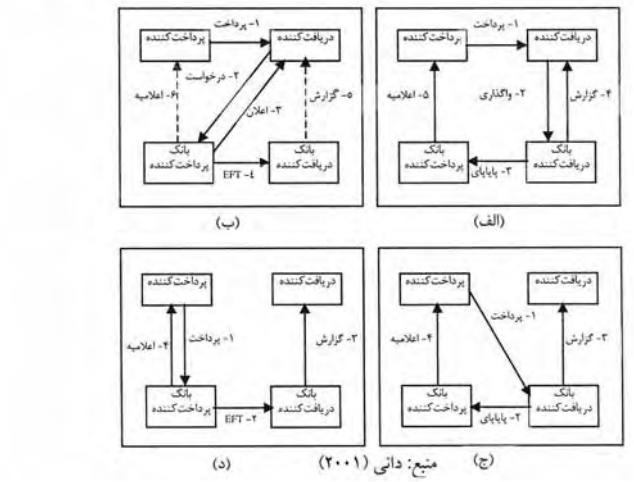
در فصل اول، مدل‌های پولی از دیدگاه مدل‌شناسی در دو دستهٔ نشانه‌ای[۲] و نوشته‌ای[۳] تقسیم شد که به ترتیب برای مدل‌های پرداختی پول‌مانند (مبتنی بر نشانه) و چک‌مانند (مبتنی بر حساب) به کار می‌روند. سیستم‌های NetCheque، VirtualPin، NetBill (دانی و همکاران، ۲۰۰۱؛ هوانگ و همکاران، ۲۰۰۱؛ شریف، ۲۰۰۰؛ وبر، ۱۹۹۸ و ۲۰۰۰)، CheckFree، RediCheck، IBM-MP[۴]، PayNow، NetChex، Agora، Polling (وبر، ۱۹۹۸؛ وبر، ۲۰۰۰)، FSTC eCheck (اندرسون، ۱۹۹۸ و ۱۹۹۹؛ دانی

---

۱. **lock box**
۲. **token-based**
۳. **notational**
۴. **IBM Micropayment**

و همکاران، ۲۰۰۱؛ اف‌اس‌تی‌سی، ۲۰۰۵؛ هوانگ و همکاران، ۲۰۰۱؛ جفی، ۱۹۹۸؛ شوتز، ۱۹۹۹؛ وید، ۱۹۹۸، ۱۹۹۹ و ۲۰۰۰؛ وبر، ۱۹۹۸ و ۲۰۰۰؛ نصیری‌مفخّم، ۱۳۸۲؛ نصیری‌مفخّم و همکاران، دی ۱۳۸۲ و ۱۳۸۳)، MANDATE II [۱] (هیدر و همکاران، ۱۹۹۹؛ مندیت، ۱۹۹۸؛ مارینید؛ میتل‌هولزر وهمکاران؛ ۱۹۹۷؛ وبر، ۲۰۰۰؛ نصیری‌مفخّم، ۱۳۸۲؛ نصیری‌مفخّم و همکاران، دی ۱۳۸۲ و ۱۳۸۳)، ABSEC [۲] (یآ و همکاران، ۲۰۰۰)، SafeCheck (دانی و همکاران، ۲۰۰۱؛ لی و همکاران، ۲۰۰۰؛ نصیری‌مفخّم ، ۱۳۸۲) و e-Check (دانی و همکاران، ۲۰۰۱؛ نصیری‌مفخّم و همکاران، دی ۱۳۸۲ و ۱۳۸۳) از ردهٔ سیستم‌های پرداخت الکترونیکی نوشته‌ای و چک‌مانند هستند که در آنها eCheck، MANDATE، SafeCheck و e-Check از نوع مدل پرداخت کلان چک‌مانند هستند که در آنها پردازش چک بر اساس سناریوهایی است که FSTC بیان کرده است.

شکل ۲-۵- سناریوهای FSTC برای پردازش چک الکترونیکی (الف) واگذاری و پایاپای (ب) نقدکردن و انتقال (ج) صندوق پرداخت (د) انتقال وجه (انتقال مستقیم وجه)



منبع: دانی (۲۰۰۱)

۱. **Managing and Administrating Negotiable Documents And Trading them Electronically**
۲. **Account Based Secure Electronic Check**

چک الکترونیکی FSTC، اولین نمونه یک خانواده اسناد مالی امضا شده به صورت رمزنگاری است، که به دلیل ویژگی‌های قابل توجه آن در ارایه خدمات جدیدی از طرف بانک‌ها به مشتریان در راستای تسهیل و کاهش هزینه‌های بالاسری تراکنش‌های مالی در حرکت از ابزارها و اسناد مالی کاغذی به سمت گونهٔ الکترونیکی دارای اهمیت است. بدین لحاظ در ادامه چک الکترونیکی FSTC را به تفصیل بررسی کرده و با سایر چک‌های الکترونیکی نیز که همگی برگرفته از چک الکترونیکی FSTC هستند، آشنا می‌شویم.

FSTC eCheck

ابداع eCheck، تلاش مشترک[۱] بیش از پانزده بانک، نهادهای دولتی، فروشندگان فنّاوری و سازمان‌های تجارت الکترونیکی سراسر دنیا، مثل: Aogrics Incorporated، بانک آمریکایی Certicom، خدمات حسابداری و مالی دفاع[۲]، خدمات مالی خزانه دولتی[۳]، Fleet bank، GTE، IBM، InteraNet، RDM Corporation، SafeNet، Sun Microsystems و خزانهٔ ایالات متحده[٤] است. eCheck نقش مهمی در آیندهٔ تجارت الکترونیکی بازی می‌کند، بطوریکه تنها مکانیزم پرداخت الکترونیکی تصدیق‌شده توسط خزانه‌داری ایالات متحده برای پرداخت‌های روی اینترنت است، و برای پرداخت‌های خزانه‌داری، در استفادهٔ فعال بوده است.

هستهٔ اولیهٔ eCheck (داگت و همکاران، US۰٥٦۷۷۹٥٥، ۱۹۹۷) در ١٤ اکتبر ۱۹۹۷ منتشر شد. در این سال، طرح‌ها برای یک یا چند برنامهٔ آزمایشی فراخوانی شد. هدف از این طرح، آزمایش چک الکترونیکی در کاربردهای واقعی در سازمان بزرگی بود که از چک‌های الکترونیکی FSTC برای پرداخت به گروهی از تولیدکنندگان کوچک تا متوسط استفاده می‌کند. این چک‌های الکترونیکی توسط بانک‌های مشارکت‌کننده در آزمایش پذیرفته می‌شد. از آنجا

---

۱. FSTC eCheck Project team: Bank One, Bank of America, Bank of Boston, Chase Manhattan, Citibank, Huntington Bank, Wells Fargo, American Express, Bank of Montreal, Bolt, Baranek, Newman, Equifax Check, Services, IBM, Intranet Inc., IRE Inc., National Semiconductor, Novell, RDM Corp., Sun Microsystems, Telequip, Unisys, Bellcore, ECCHO, NACHA, NY Clearing House, Oak Ridge Nat'l Laboratory, Sandia National Laboratory, U. of Southern California.

۲. Defense Finance & Accounting Service

۳. Federal Reserve Financial Services

٤. United States Treasury

که پروژهٔ eCheck از اهداف اصلی FSTC فراتر رفت، برای بسط این فنّاوری در ماورای جامعهٔ بانکداری، در ۱۹۹۹ مدیریت eCheck اولیه از FSTC به CommerceNet منتقل شد (ابراژویچ، ۲۰۰۱-۱؛ اندرسون، ۱۹۹۸؛ کامرس‌نت، ۲۰۰۵؛ ای‌چک، ۲۰۰۵؛ ای‌چک‌ورلدواید، ۲۰۰۱، ۲۰۰۱k و ۲۰۰۵؛ گلیناس، ۲۰۰۱؛ جفی، ۱۹۹۸؛ شوتز، ۱۹۹۹؛ وید، ۱۹۹۸؛ نصیری‌مفخّم، ۱۳۸۲).

تلاش فاز ۱ بازار خزانهٔ آمریکا در سال ۲۰۰۰ با ۱۰،۰۰۰،۰۰۰$ پرداخت امن توزیع شده روی اینترنت با موفقیت از کار در آمد. نسخه‌های بعدی آن (اندرسون و همکاران، US۰٦۰۲۱۲۰۲، ۲۰۰۰ و US٦۲۰۹۰۹۵، ۲۰۰۱) در ۱ فوریه ۲۰۰۰ و ۲۷ مارس ۲۰۰۱ صادر شدند. فاز ۲، تا هنگامیکه جامعه مشارکت‌کنندگان برون‌مرزی پیدا کند، باز است. FSTC eCheck دومین بستر آزمایشی خود را در خارج از آمریکا، در آگوست تا ۱۲ نوامبر ۲۰۰۱ تحت پروژهٔ just٤Dental در بازار تجهیزات دندانپزشکی استرالیا سپری کرد (ای‌چک، ۲۰۰۵؛ ای‌چک‌ورلدواید، ۲۰۰۵؛ ای‌چک‌ورلدواید، ۲۰۰۲؛ ای‌چک‌ورلدواید، ۲۰۰۱؛ گلیناس، ۲۰۰۱؛ نصیری‌مفخّم، ۱۳۸۲).

eCheckها به واسطهٔ FSML[1] و امضاهای دیجیتالی، در زمرهٔ امن‌ترین ابزارهای پرداخت تهیه شده تا این لحظه هستند و از جایگاه ویژهٔ تکنیک‌های امنیتیِ هویت‌شناسی، رمزنگاری کلید عمومی، امضاهای دیجیتالی، مراجع گواهیِ، تشخیص تکراری‌ها و رمزنگاری بهره می‌گیرند. جزئیات اطلاعات و ویژگی‌های امنیتی درون‌ساخت چک الکترونیکی، بانک‌ها را قادر به تصدیق و پردازش خودکار می‌کند و به کاربران چک الکترونیکی توانایی حفاظتی بیشتری در برابر تقلب چک که با چک‌های کاغذی امکان دارد، می‌دهد (کلیسنز و همکاران، ۲۰۰۱؛ اف‌اس‌ام‌ال، ۱۹۹۹؛ شیموس، ۲۰۰۲؛ شریف، ۲۰۰۰؛ وایز، ۲۰۰۱؛ نصیری‌مفخّم، ۱۳۸۲).

امضاهای دیجیتالی اثبات می‌کنند که سفارش پرداخت را فقط و فقط شخص پرداخت‌کننده داده است و با اطمینان دادن از جامعیت پیام،

---

۱. Financial Services Markup Language

FSML (اندرسون و همکاران، ۲۰۰۰؛ اف‌اس‌ام‌ال، ۱۹۹۹؛ اف‌اس‌تی‌سی، ۱۹۹۹؛ نصیری‌مفخّم، ۱۳۸۲) که توسط SGML ISO ۸۸۷۹ تعریف می‌شود برای حمایت از ساختارهای داده‌ای و امضاهای دیجیتالی مورد نیاز برای echeckها طراحی شد و در آن، ساختار و اقلام داده‌ای سند به صورت بلوک‌هایی برای echeckها با برچسب‌هایی از هم مجزا می‌شوند.

هویت‌شناسی، و نفی‌انکار، eCheck را در برابر تقلب امن می‌کنند. اکنون بانک‌ها بررسی‌های دقیقی را روی چک‌های کاغذی برای بررسی اصلی یا تکراری بودن چک‌ها انجام می‌دهند. این موضوع در مورد چک‌های الکترونیکی کاملاً جدی عمل می‌شود، بطوریکه قابلیت‌های قوی‌تری برای پیشگیری و شناسایی تکراری‌های جعلی یا اشتباهی ارایه می‌دهد.

تقلب یک امضای دیجیتالی می‌تواند توسط هر کسی که کلید محرمانهٔ امضای فرد امضاکننده را دارد، ساخته شود. برای حفاظت کلید محرمانهٔ امضای امضاکننده از سرقت و سوءاستفاده، از کارت هوشمند[1] (اندرسون ۱۹۹۹؛ چان و همکاران، ۲۰۰۱؛ گلیناس، ۲۰۰۱؛ امرایهی و همکارَان، ۲۰۰۱؛ شوتز، ۱۹۹۹؛ شریف، ۲۰۰۰؛ وید، ۱۹۹۸، ۱۹۹۹ و ۲۰۰۰؛ نصیری‌مفخّم، ۱۳۸۲) دسته‌چک الکترونیکی استفاده می‌شود. کلید محرمانهٔ امضاکردن فقط از درون کارت هوشمند[2] توسط الگوریتم‌های رمزنگاری که مطابق استانداردهای صنعت بانکداری است، تولید و استفاده می‌شود. کلید محرمانهٔ امضا کردن هرگز به کامپیوتر امضا کننده منتقل و افشا نمی‌شود تا از طریق ارتباط شبکه‌ای کامپیوتر مورد سرقت واقع شود. دسته چک الکترونیکی همچنین بطور خودکار هر چک را امضا ، به منظور اطمینان از یکتایی چکها شماره‌گذاری می‌کند، و یک log یا ثبت چک را نگهداری می‌کند، تا در مواردی‌که امضا، پشت‌نویسی، یا واگذاری چک داده شده نفی شود به کمک گرفته شود. استفاده از دسته چک الکترونیکی، با ورود یک PIN[3] توسط امضاکننده کنترل می‌شود. این امر به دریافت‌کنندگان و بانک‌ها اطمینان می‌دهد که پرداخت‌کنندگان قانونی، روی کلیدهای محرمانه امضای خود مالکیت وکنترل دارند.

دسته چک الکترونیکی (شکل ۲-٦) با استفاده از رویه‌هایی براساس فرآیندهای صدور کارت بانکی، آماده می‌شود (شکل ۲-۷). کلید عمومی صادر

۱- یک کارت هوشمند، یک کارت پلاستیکی حاوی یک تراشهٔ کامپیوتری است که مقادیر زیادی از اطلاعات را نگه می‌دارد و برخی پردازش‌ها را انجام می‌دهد و در مقابل تغییرات خیلی مقاوم است. کارت‌های هوشمند برای تأمین حافظهٔ امن کلیدهای خصوصی امضا و برای ایجاد و صحت سنجی امضاهای دیجیتالی یا چک‌های الکترونیکی مناسب هستند.

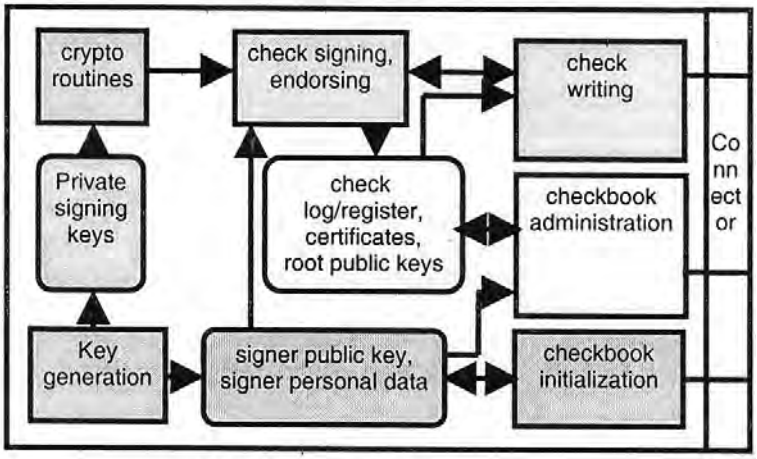
۲ــ این دسته چک الکترونیکی براساس نرخ تراکنش‌های دارندهٔ آن، می‌تواند به صورت کارت‌های هوشمند، کارت‌های PCMCIA در کامپیوترهای کیفی، یا سخت‌افرار رمزنگاری متصل به سرورها باشد. برای دریافت‌کنندگانی که می‌خواهند eCheck را پشت‌نویسی و فقط در بانک خود واگذار کنند، از پیاده‌سازی‌های صرفاً نرم‌افزاری می‌تواند استفاده شود.

۳. Personal Identification Number

شده از کارت، شامل یک گواهی X.۵۰۹ امضا شده توسط مرجع گواهی بانک و مربوط به یک بلوک حساب است که آن هم توسط مرجع گواهی بانک امضا شده است. سرورهای eCheck بانک همچنین پایگاه داده مستقلی از کلیدهای عمومی امضاها را نگه می‌دارند، به طوری که آنها همیشه آخرین روابط کلیدها با حساب‌ها و امضاکنندگان را می‌دانند.

هر کدام از سیستم‌های پرداخت‌کننده و دریافت‌کننده برای صدور echeck ها و واگذاری آنها در اولین بانک محل واگذاری و بانک پرداخت‌کننده باید عملکردهای خاصی داشته باشند، که در شکل‌های ۲-۸ تا ۲-۱۱ آمده است[۱].

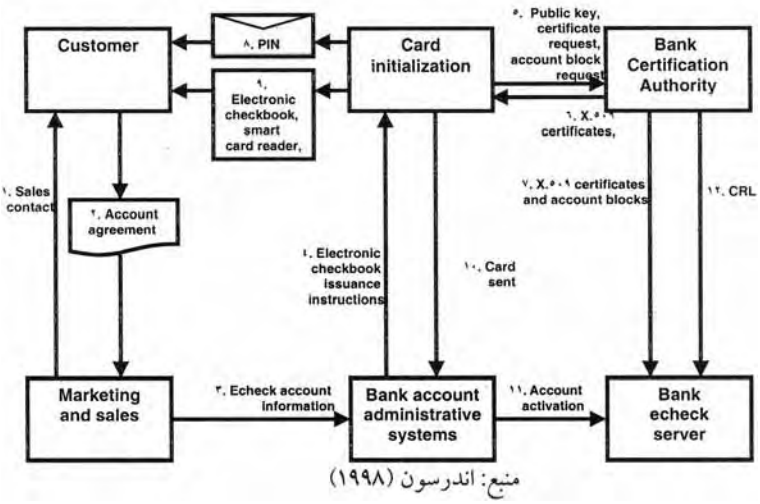
شکل ۲-٦- توابع کارت دسته چک الکترونیکی



منبع: اندرسون (۱۹۹۸)

۱ـ به خوانندهٔ علاقمند، مطالعهٔ (اندرسون، ۱۹۹۸و ۱۹۹۹؛ وید، ۱۹۹۸؛ نصیری‌مفخّم، ۱۳۸۲) توصیه می‌شود.

شکل ۲-۷- توزیع دسته چک الکترونیکی وزیرساختار کلید



منبع: اندرسون (۱۹۹۸)

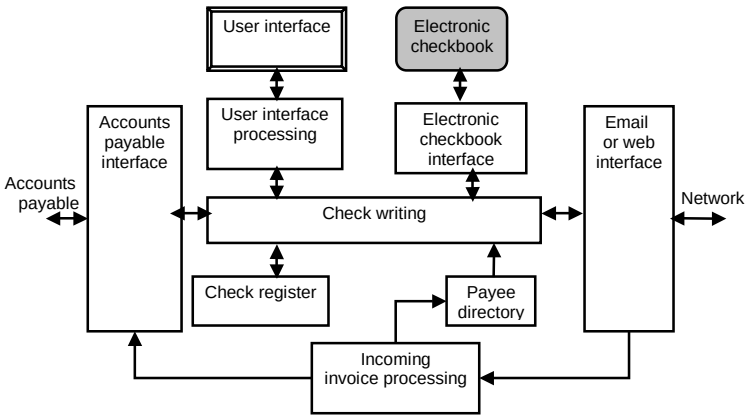
بانک‌هایی که حساب‌های چک الکترونیکی را ارایه میدهند، باید اعضایی از یک سازمان (مثلاً ECCHO[1]) یا اتاق پایاپایی باشند که قوانین تسویه و پایاپای فراهم می‌کند، یا با تسویه و پایاپای echeckها بصورت دوطرفه توافق داشته باشند. همچنین شبکه‌های دیگری، همچون اتاق پایاپای خودکار (ACH[2]) می‌تواند برای انتقال وجوه بین بانک‌ها مورد استفاده فرا گیرد (اندرسون، ۱۹۹۸ و ۱۹۹۹؛ نصیری‌مفخّم، ۱۳۸۲؛ نصیری‌مفخّم و همکاران، ۱۳۸۳).

---

۱. Electronic Check Clearing House Organization

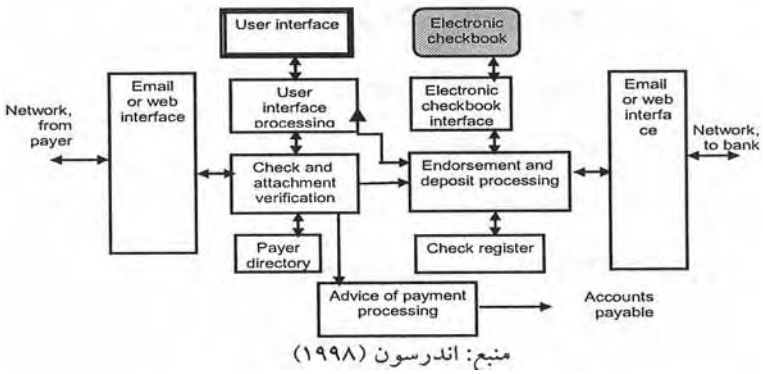
۲. Automated Clearing House

شکل ۲-۸- سیستم پرداخت‌کننده



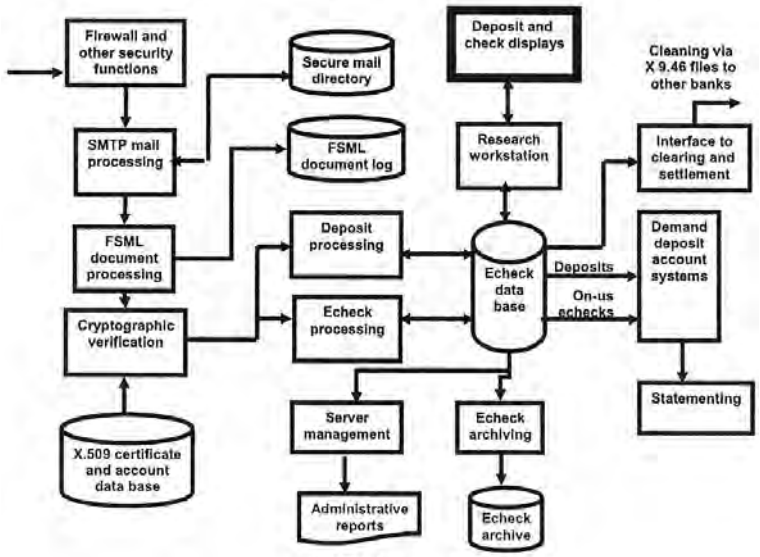
منبع: اندرسون (۱۹۹۸)

شکل ۲-۹- سیستم دریافت کننده



منبع: اندرسون (۱۹۹۸)

شکل ۲-۱۰- توابع سرور بانک اولین واگذاری echeck



منبع: اندرسون (۱۹۹۸)

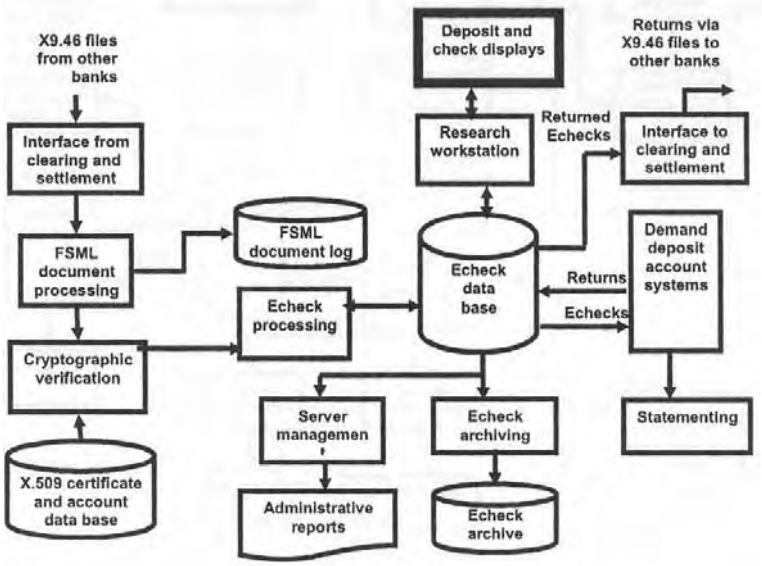
MANDATE II

MANDATE I که اساس آن از پروژه‌ای تحت برنامهٔ EC TEDIS (۱۹۹٤) برای انتقال الکترونیکی اسناد گرفته شد، پروژه‌ای توسط شرکت دانمارکی Cryptomatic با حمایت ETS[1] است، که در آن با نسخه‌برداری از عملکرد چک کاغذی، یک چک الکترونیکی با استفاده از زیرساختار کلید عمومی، برای استفاده B۲B جامعهٔ اروپایی به صورت پروتوتایپ در ۱۹۹۹ با حمایت مالی کمیسیون اروپایی INFOSEC پیاده‌سازی شده است. هدف این پروژه، بکارگیری کارت‌های هوشمند برای استفاده از امضاها و گواهی‌های دیجیتالی جهت صدور چک‌های الکترونیکی و ارسال از طریق پست الکترونیکی است. عملکرد آن، برگرفته از چک الکترونیکی FSTC است، به جز آنکه به دلیل تبعیت از فرهنگ و قانون چک در اروپا، قابلیت انتقال و پشت‌نویسی چک‌ها برای غیر، جزء ویژگی‌های ثانویه‌ای است که در این پروژه در مورد آن بحث می‌شود. از طرف دیگر، نکتهٔ دیگری که در چک الکترونیکی FSTC (باز به دلیل تبعیت از فرهنگ و قانون چک در آمریکا) به آن اشاره نشده بوده، قابلیت بازیابی چک‌هایی است که پس از صدور و قبل از ارسال از دست رفته‌اند. برای تسویهٔ

۱. European Trusted Services

چک‌ها نیز در نظر داشتند که از تراکنش‌های BACS EFS (همچون بدهکاری مستقیم) بین بانک‌های بریتانیا و برای بعد بین‌المللی از تجمیع با SWIFT[1] استفاده کنند (چان و همکاران، ۲۰۰۱؛ سوئیفت؛ ۲۰۰۵؛ وید، ۱۹۹۸؛ نصیری‌مفخّم، ۱۳۸۲). همچنین در چک الکترونیکی FSTC، امکان تجدید الکترونیکی دسته‌چک‌های الکترونیکی که MANDATE به آن می‌پردازد، در نظر گرفته نشده بود. برای مرحلهٔ آزمایشی پیاده‌سازی، سه بانک از سه کشور متفاوت اروپایی، Royal Bank (اسکاتلند، بریتانیا)، ING Bank (هلند)، و Nordvestbank (دانمارک) مشارکت داشتند.

شکل ۲-۱۱- توابع سرور echeck بانک پرداخت کننده



منبع: اندرسون (۱۹۹۸)

۲-۳-۳ SafeCheck

۱. Society for Worldwide Intertbank Financial Telecommunication

SafeCheck (۲۰۰۰) توسط «جائه کیو لی» و «هانگ سئونگ یون» از مؤسسهٔ عالی علوم و تکنولوژی کشور کُره ارایه شده و بر اساس اعتبار صادرکنندهٔ چک، سه نوع خدمات در نظر می‌گیرد:

- مجازشناسی فقط در موقع صدور دسته چک (با امکان ماندهٔ بدهکاری[۱]).
- مجازشناسی به هنگام صدور هر چک، علاوه بر مجازشناسی اولیه موقع صدور چک (با امکان ماندهٔ بدهکاری).
- صدور چک فقط در حد موجودی حساب.

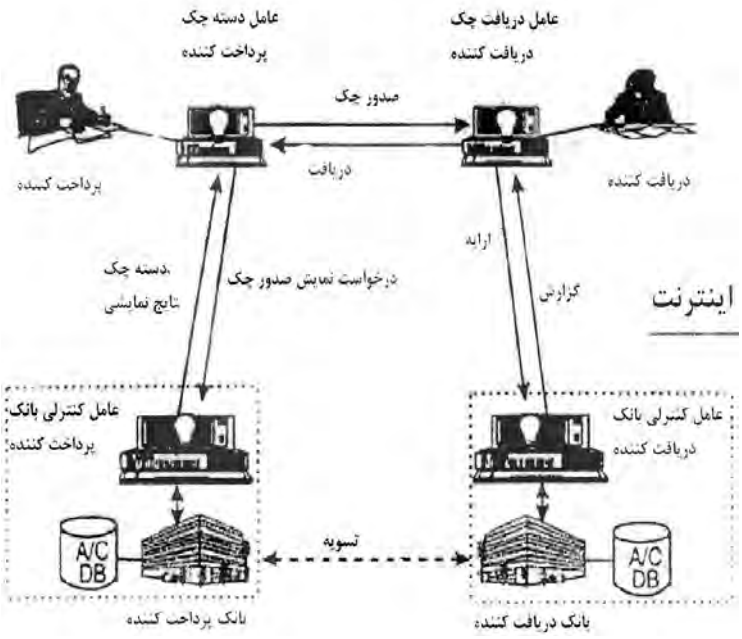
SafeCheck وضعیت را بررسی کرده و برای پرهیز از استفادهٔ نادرست، بانک‌های پرداخت‌کننده و دریافت‌کننده می‌توانند به روشی توزیع شده، اطلاعات مرتبط با دسته چک الکترونیکی پرداخت را کنترل و صدور چک‌های غیرمجاز را بلوک کنند. SafeCheck به طور خودکار مبلغ صادرشده را از حساب پرداخت‌کننده در موقعی که پرداخت‌کننده مبلغ برداشت را تأیید می‌کند، برداشت کرده و به حساب دریافت‌کننده واریز می‌نماید. در این سیستم از رمزنگاری کلید عمومی، امضای دیجیتالی و گواهی استفاده می‌شود. همانگونه که در شکل ۲-۱۲ نشان داده شده است، سیستم SafeCheck از سه عامل هوشمند تشکیل گردیده که عبارتند از: (۱) عامل دسته چک در سمت صادرکنندهٔ چک (که اصل عامل دسته چک می‌تواند در کارت هوشمند ذخیره شود)، (۲) عامل دریافت‌کنندهٔ چک در سمت دریافت‌کنندهٔ چک، و (۳) دو عامل کنترل بانک در بانکهای صادرکننده و دریافت‌کننده

---

۱. overdraft

ویژگی عامل‌ها[1]، استقلال، توانایی ارتباط، استدلال و قابلیت یادگیری است. مبادله پیام‌ها به صورت KQML[2] روی پروتکل TCP/IP انجام می‌شود و عاملها روی چهار کامپیوتر متصل از طریق اینترنت با هم ارتباط دارند. در سیستم پروتوتایپ، تسویه ارایه شده توسط عامل دریافت‌کننده چک، مستقیماً online بین عاملهای کنترلی دو بانک صورت می‌گیرد (لی و همکاران، ۲۰۰۰؛ نصیری‌مفخّم، ۱۳۸۲).

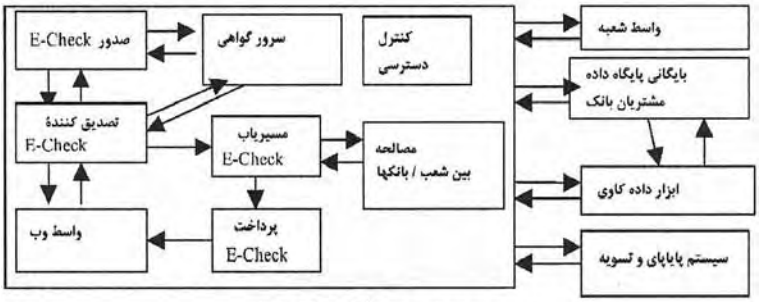
شکل ۲-۱۲- معماری سیستم SafeCheck



۱ ـ در MAGMA (Minnesota Agent Marketplace Architecture) و PIPEMART (Practical Interactive and Personizable MARkeTplace) نیز به کار رفته‌اند.

۲. Knowledge Query and Manipulation Language

شکل ۲-۱۳- معماری سیستم E-Check



منبع: دانی و همکاران (۲۰۰۱)

۲-۳-٤ E-Check

E-Check (۲۰۰۱) که توسط انستیتوی تحقیق و توسعه فنّاوری بانکداری هندوستان ارایه شده نیز مدلی است که بر اساس مدل چک الکترونیکی FSTC برای هندوستان در دست پیاده‌سازی است. پرداخت‌کننده، دریافت‌کننده، بانک پرداخت‌کننده، بانک دریافت‌کننده و اتاق پایاپای، مؤلفه‌های معماری E-check ارائه شده هستند. سیستم E-check برای حساب‌های مشتریان متمرکز در یک بانک تعریف شده است. دفترچه E-check که توسط بانک صادر می‌شود روی یک فلاپی یا کارت هوشمند بارگذاری می‌شود. یک PIN نیز برای بازکردن قفل فلاپی/کارت هوشمند توسط بانک داده می‌شود که بعداً می‌تواند توسط مشتری عوض شود. موقع نوشتن چک، مشتری باید فلاپی/کارت هوشمند را وارد کرده و قفل آنرا با PIN باز کند. با استفاده از زوج کلیدهای عمومی و خصوصی در کارت هوشمند، E-check می‌تواند بصورت Off-Line ایجاد و امضا شود. بدین طریق (بدون تحمیل هویت شناسی On-Line) امنیت مناسبی فراهم می‌شود. این سیستم به از دست رفتن E-check ها نیز اهمیت می‌دهد، چون اگر فلاپی/ کارت هوشمند گم شود، پرداخت‌کننده می‌تواند برای باقیمانده چک‌ها درخواست توقف پرداخت به بانک بدهد و درخواست دفترچه E-check جدید بکند (دانی و همکاران، ۲۰۰۱؛ نصیری‌مفخّم، ۱۳۸۲).

جدول ۲-۱- مقایسه سیستمهای پرداخت الکترونیکی

ویژگیها	پرداخت online کارت اعتباری (SET)	پول الکترونیکی در کارت هوشمند (Mondex)	چک الکترونیکی (FSTC)
زمان واقعی پرداخت	پرداخت بعدا	پیش‌پرداخت	پرداخت بعدا
انتقال اطلاعات تراکنش	فروشگاه و بانک وضعیت کارت اعتباری را بررسی می کنند	کارتهای هوشمند دو طرف انتقال را انجام می‌دهند	چکهای پیا دستور پرداخت الکترونیکی بایید پشت‌نویسی شوند
Online و Offline	تراکنشهای online	تراکنشهای online و انتقالهای offline مجاز هستند	انتقالهای offline مجاز است
با دخالت حساب بانکی	پرداخت از حساب کارت اعتباری انجام می‌شود	پرداخت بدون دخالت و از حساب کارت هوشمند انجام می‌شود	پرداخت از حساب بانکی انجام می‌شود *
کاربران	هر کاربر قانونی کارت اعتباری	هر کسی دارای حساب بانکی یا حساب کارت اعتباری	هر کسی که حساب بانکی دارد
طرفی که به او پرداخت می‌شود	بانک توزیع کننده	فروشگاه	فروشگاه
خطر تراکنش برای مشتری	پیشتر خطر توسط بانک توزیع کننده تحمل می‌شود، مصرف کنندگان فقط متحمل بخشی از خطر می گردند	مشتری در خطر است که کارت هوشمند حاوی پول الکترونیکی دزدیده، مفقود، یا سوءاستفاده شود	مشتری اکثر خطر را متحمل می‌شود، اما می‌تواند در هر موقعی، پرداخت را متوقف کند
درجهٔ فعلی عمومیت	بسرخلاف سایر روشهای پول الکترونیکی، سازمانهای کارت اعتباری برای گواهی بررسی می کنند سپس خریدها را جمع آوری می کنند. بنابراین، می‌توانند به صورت بین‌المللی استفاده شود، و در حال پیداکردن استفادهٔ گسترده‌تری است		نمی‌تواند استانداردهای بین‌المللی را برآورده کند، بنابراین خیلی عمومیت ندارد
اختفا (ناشناسی)	جزئا یا کلا ناشناس	کاملا ناشناس، اما اگر لازم باشد، نمایندگی پردازش مرکزی می‌تواند از فروشگاه اطلاعاتی دربارهٔ مشتری بخواهد	بدون اختفا
پرداختهای کوچک	هزینه تراکنشها بالاست. برای پرداختهای کوچک مناسب نیست	هزینه تراکنشها پایین است. فروشگاهها می‌توانند بدهی‌ها را جمع کرده تا به حدی برسد که برای آن پرداخت شود. بنابراین برای پرداختهای کوچک مناسب است.	فروشگاهها می‌توانند بدهی‌ها را جمع آوری کرده تا به یک حدی برسد که برای آن پرداخت شود. برای پرداخت‌های کوچک مناسب است
محافظت پایگاه داده‌ای	محافظت از اطلاعات حساب عادی کارت اعتباری	برخلاف سایر روشهای پول الکترونیکی که مستلزم نگهداری پایگاه دادهٔ بزرگی از رکوردهای شماره سریال پولهای الکترونیکی استفاده شده است، فقط محافظت از اطلاعات عادی حساب لازم است.	محافظت از اطلاعات حساب عادی
ارزش صوری اطلاعات تراکنش	می‌تواند در تطابق با محدوده، امضا و صادر شوند	برخلاف سایر روشهای پول الکترونیکی که ارزش صوری اغلب تنظیم شده است و تغییر نمی‌پذیرد، می‌تواند به سادگی در تطابق با محدوده کسر شود	می‌تواند در تطابق با محدوده، امضا و صادر شوند
دنیای واقعی/مجازی	جزئا می‌توانند در دنیای واقعی استفاده شوند	می‌توانند در دنیای واقعی و مجازی استفاده شود	محدود به دنیای مجازی است، اما می‌تواند با یک حساب جاری در دنیای واقعی مشترک باشد
محدودیت برای مقادیر انتقالی	وابسته به محدوده کارت اعتباری	وابسته به مقدار پولی است که پیش‌پرداخت و ذخیره شده است	بدون محدوده
جابجایی	بله	برخلاف سایر پولهای الکترونیکی که در کامپیوتر کاربر ذخیره می‌شوند، قابل جابجایی است.	خیر

* مزیت برای کمک به نظام نقدینگی

منبع: پو و همکاران (۲۰۰۳)

در سیستم پروتوتایپ، به‌دلیل اتصال ضعیف بین بانک مادر و بعضی از شعبه‌هایش، دفترچه E-check به صورت on-Line صادر نمی‌شد و فقط برای یک بانک طراحی شده بود، به طوری که لازم است پرداخت‌کننده و دریافت‌کننده در یک بانک حساب داشته باشند. در این سیستم هیچ پایاپای بین بانکی و رسیدگی خودکار به چک‌های الکترونیکی از طریق اینترنت وجود نداشت. پس از آن، پروژهٔ دیگری در حال انجام است که مبتنی بر XML و برای حمایت از محیط بانکی با شعبات توزیع شده و پایاپای و تسویه بین‌بانکی است (شکل ۲-۱۳).

۲-٤ مقایسهٔ سیستم چک الکترونیکی با سایر سیستم‌های پرداخت الکترونیکی

در ردهٔ پرداخت‌های کلان چک الکترونیکی، تنها دو سیستم چک الکترونیکی FSTC و MANDATE به سطح پروتوتایپ عملی یا آزمایشی

رسیده‌اند. این دو سیستم، تشابه بسیاری دارند به جز آنکه MANDATE، قابلیت بازیابی چک‌هایی که پس از امضا و قبل از ارسال از دست رفته‌اند را نیز مورد توجه قرارداده است (مثلاً کارت امضا، قبل از اقدام برای ارسال به دریافت کننده، تخریب یا غیرقابل استفاده شده باشد). MANDATE بیان می‌کند که پس از آنکه کاربر این نسخه را به بانک ارسال کرد، بانک پس از سپری شدن مدت اعتبار واگذاری چک، چنانچه چکی با این ویژگی برای پرداخت‌شدن دریافت نکند، مبلغ مندرج روی چک جهت بدهکاری پرداخت‌کننده را به حساب وی برمی‌گرداند. مشاهده می‌شود که این حالت مشابه آن است که برگی از چک موقع نوشتن مخدوش شده باشد و بدون استفاده برای پرداخت، از دست رفته باشد. در این حالت، صرفاً یک شماره از تعداد چک‌های قابل استفاده کمتر می‌شود، و موقع صدور چک و قبل از ارسال آن، هیچ بدهکاری به حساب مشتری تا موقع واگذاری دریافت‌کننده توسط بانک دریافت‌کننده در بانک پرداخت‌کننده صورت نمی‌گیرد که مستلزم بازیابی وضعیت حساب پرداخت‌کننده باشد[1]. لذا این ویژگی MANDATE کاربرد پیدا نمی‌کند. ضمناً FSTC از نظر مرحلهٔ عملیاتی، در فاز جلوتری از MANDATE است. در جدول ۲-۱، ویژگی‌های دو سیستم معروف SET و Mondex را که در فصل اول بیان گردیدند، با ویژگی‌های چک الکترونیکی FSTC مقایسه گردیده است چنانچه مشاهده می‌شود، برخلاف کارت اعتباری و پول الکترونیکی که مبلغ محدودی را می‌توان توسط آنها انتقال داد، در چک الکترونیکی محدویتی نیست و همین ویژگی، آن را برای پرداخت‌های کلان بازرگانی شرکت‌ها و دولت مناسب می‌کند. ویژگی پرداخت از حساب بانکی در چک‌های الکترونیکی، مزیت این ابزار و در راستای کمک به بهبود نقدینگی است. در مورد کارت‌های هوشمند پول الکترونیکی، گم شدن کارت برابر با گم شدن پول است، درحالیکَه در مورد چک‌های الکترونیکی، پول در بانک است. از طرفی اطلاعات کارت اعتباری از سوی هر کسی که آن را بیابد قابل سوءاستفاده است و تراکنش‌ها می‌تواند از سوی هر کدام از طرفین انکار شود.

تجارت و پرداخت الکترونیکی و بانکداری الکترونیکی در ایران

۱ـ این ویژگی، به نوعی مشابه قانون ۲۶۱ قانون تجارت در مورد برات است.

در ایران، با تدوین قوانین تجارت الکترونیکی در کشور و عضویت در AFACT[1] و WIPO[2]، مقدمات ورود به صحنهٔ جهانی فراهم شده است، به طوری که میزان صرفه‌جویی ارزی حاصل از بکارگیری تجارت الکترونیکی در تجارت خارجی در سال‌های برنامه سوم، ۵۸/۹۸ هزار میلیارد ریال خواهد بود. ایران برای ورود به صحنهٔ تجارت جهانی بایستی اصلاحات سیستم پرداختی خود را مد نظر قرار دهد، ولی هنوز موانع و چالش‌هایی برای پرداخت الکترونیکی وجود دارد. در سال‌های اخیر، همگام با گسترش روزافزون تجارت الکترونیکی در اقتصاد جهانی، کاربرد فنّاوری اطّلاعات و ارتباطات در حوزهٔ مبادلات پولی و مالی نیز افزایش یافته و بانک‌ها در اثر وجود فشارهای رقابتی در بازارهای مالی، با حرکت به سوی بانکداری الکترونیکی و عرضه خدمات مالی نوین، نقش شایان توجهی در افزایش حجم تجارت الکترونیکی داشته‌اند.

شکل ۲-۱۴- جایگاه سیستمهای اتوماسیون

منبع: نیکبخش تهرانی و همکاران (۱۳۸۰)

سوئیفت و اتوماسیون سیستم بانکی در ایران

امروزه نقش مؤثر شبکه‌های مخابراتی پیشرفته، ایمن و با سرعت بالا در عملیات سریع و مکانیزه تبادل پیام‌های بین بانکی و بانکداری بین‌المللی بر کسی پوشیده نیست. شبکه مخابراتی سوئیفت جهانی، یکی از این شبکه‌های

۱. Asia Pacific EDIFACT Council for Trade Facilitation and Electronic Business
۲. World Intellectual Property Organization

اختصاصی است که در حال حاضر تبادل اطلاعات عملیات ارزی بین بانکی را تحت قالبی استاندارد امکان پذیر ساخته است (چان و همکاران، ۲۰۰۱؛ شیموس، ۲۰۰۲؛ شریف، ۲۰۰۰؛ سویفت، ۲۰۰۵؛ سازمان ملل، ۲۰۰۱؛ نیکبخش تهرانی و همکاران، ۱۳۸۰؛ نصیری‌مفخّم، ۱۳۸۲).

جایگاه سیستم‌های اتوماسیون

در ایران، بر اساس مصوبه مجمع عمومی بانک‌ها در سال ۱۳۷۲، طرح جامع اتوماسیون سیستم بانکی با مسئولیت مشاور اجرایی ریاست بانک مرکزی با اهداف «کاهش مشکلات اجرایی در شعب و ادارات مرکزی بانک‌ها و افزایش توان اجرایی سیستم»، «تسریع در اجرای عملیات نظام بانکی و ارتقای کیفیت آن»، «ایجاد زمینه لازم برای کاهش مبادلات نقدی و نقل و انتقال پول»، «ایجاد امکان دسترسی به اطلاعات به هنگام، برای اتخاذ تصمیم در مورد سیاست‌های پولی و بانکی»، «صرفه جویی در وقت کارکنان و مشتریان بانک‌ها، کاهش نقل و انتقال فیزیکی مدارک در شعب، کاهش سفرهای شهری و ...»، و «ایجاد هماهنگی لازم برای ارتباط با بانک‌های خارج از کشور» شکل گرفت (شکل ۲-۱٤). ضمناً معیارهایی همچون «قطع وابستگی جغرافیایی مشتریان به شعب خاص»، «گسترش ارایه خدمات بانکی به خارج از ساعات کار رسمی بانک»، «محور قراردادن مشتری در مبادلاتش با بانک (و نه حساب‌های مشتری)»، «حفظ یکپارچگی اطلاعات بانک و اجتناب از ذخیره چندباره و زاید اطلاعات» و «استفاده از تکنولوژی‌های اثبات شده» برای این طرح ذکر گردید (نیکبخش تهرانی و همکاران، ۱۳۸۰).

بر این اساس، بانک‌های جمهوری اسلامی ایران نیز پس از نصب تجهیزات مورد نیاز، در سال ۱۳۷۲ به عضویت این سازمان بین‌المللی درآمدند و توانستند از مزایای این شبکه جهانی در ارایه خدمات سریع به مشتریان خود بهره گیرند. همچنین بسیاری از بانک‌ها با نصب دستگاههای خودپرداز و صدور کارت‌های پیش‌پرداخت، گام مؤثری در بهبود ارایه خدمات بانکی در کشور برداشتند.

شتاب، پایاپای ریالی بین بانکی مکانیزه

شبکهٔ بانکی کشور تاکنون مبادلات ارزی خود را از طریق سوئیفت، به عنوان بزرگترین و امن‌ترین شبکهٔ ارتباطات مالی جهانی، به انجام می‌رساند،

ولی برای مبادلات ریالی بین بانکی، فاقد سوئیچی امن برای پایاپای ریالی بین بانکی در کشور بود و کارت‌های پرداخت بانک‌ها با هم ناسازگار بودند، اما با شکل‌گیری مرکز شتاب (شبکه تبادل اطلاعات بین بانکی) (شتاب، ۱۳۸۳)، بانکداری الکترونیکی در ایران وارد مرحلهٔ نوینی گردیده است.

مطابق نگارشی که در خرداد ۱۳۸۱ از پیش‌نویس مقررات حاکم بر این مرکز داده شده است (کیانی و همکاران، ۱۳۸۱)، شتاب، مجموعهٔ استانداردها، مقررات، رویه‌ها، نرم‌افزارها و سخت‌افزارهایی است که بسترهای لازم را به منظور تبادل اطلاعات، تهاتر و تسویه تراکنش‌های کارت‌های پرداخت صادر شده توسط اعضا، فراهم می‌سازد. از جمله وظایف این مرکز، دریافت و پردازش اطلاعات کارت‌ها، تهاتر و ارسال پیام‌های تسویه برای نگهدارنده حساب‌ها، تهیه و ارسال تأییدیه‌ها و گزارش‌ها، و ایجاد ارتباط با مراکز بین‌المللی است.

کارت‌های بانکی، نقش مهمی را در گردش عملیات پولی در سطح ملی و بین‌المللی ایفا می‌نمایند. با افزودن خدمات شتاب به سبد خدمات بانکی، این امکان با استفاده از کارت پرداخت فراهم است که در تمامی ساعات شبانه روز، علاوه بر دریافت خدمات از بانک صادر کننده کارت، بتوان از طریق دستگاه‌های خود پرداز (ATM) و پایانه‌های فروش (POS) نصب شده در مراکز ارایه کالا و خدمات نیز اقدام نمود. بر این اساس کارت پرداخت بانک‌های عضو شتاب تمام انتظاری را که از یک حساب پیشرفته امروزی می‌رود، برآورده می‌سازد. صرفه جویی در وقت، برخورداری از ویژگی‌های امنیتی، برداشت پول از حساب کارت، حواله الکترونیکی، واریز پول به حساب کارت، دریافت مانده موجودی و صورت حساب از مزایای شتاب است[۱].

۲-۵-۳ سیاست‌های اجرایی تجارت الکترونیکی جمهوری اسلامی ایران

نظر به گریزناپذیر بودن استفاده از تجارت الکترونیکی در حفظ، تقویت و توسعه موقعیت رقابتی کشور در جهان، طرح توجیهی و سیاست تجارت الکترونیکی جمهوری اسلامی ایران در ۱۸ بند تنظیم گردید، و مواردی از آن

۱. برای اطلاعات بیشتر به (شتاب، ۱۳۸۳) و پیوست چهارم از (نصیری‌مفخّم، ۱۳۸۳) مراجعه کنید.

که به موضوعات مطرح در بانکداری نوین مرتبط هستند، به شرح زیر است (کمیته ملی ادیفاکت ایران، ۱۳۸۰)[۱]:

بند ۱. شرکت مخابرات موظف است ضمن تسهیل و بهره‌گیری از مشارکت بخش غیردولتی در این زمینه، حداکثر تا پایان سال ۱۳۸۱ نسبت به تامین و راه‌اندازی سخت‌افزار و نرم‌افزارهای موردنیاز و برقراری خطوط ارتباطی پرسرعت و مطمئن به شبکه اینترنت در محدوده فعالیت خود اقدام و هزینه استفاده از خطوط مزبور را کاهش‌دهد، بطوریکه ظرفیت پهنای باند دیتای کل کشور، تعداد کاربران اینترنتی، و تقسیمات خطوط شبکه را به ترتیب از Mbit ۱۰۰۰، ۱۵۰۰۰۰۰، و ۳٤K در سال ۸۰ به Gbit ۵، ۵۰۰۰۰۰۰، و K ۱۵۵ در سال ۸۱ برساند.

بند ۲. جمع عمومی بانک‌ها، بانک مرکزی و شورای‌عالی بانک‌ها موظفند تا پایان سال ۱۳۸۱ بسترهای سخت افزاری و عملیاتی لازم را برای راه‌اندازی و بکارگیری وسیع انتقال الکترونیکی وجوه براساس طرح مصوب سال ۱۳۸۰ در کمیسیون تخصصی اطلاع رسانی اقتصادی، بازرگانی و تجارت الکترونیکی، فراهم نماید.

بند ۳. مجمع عمومی بانک‌ها، بانک مرکزی و شورای‌عالی بانک‌ها موظفند تا پایان سال ۱۳۸۱ امکان صدور، بکارگیری و فراهم‌نمودن خدمات کارت‌های اعتباری را در کشور فراهم نماید.

بند ٤. وزارت بازرگانی موظف است حداکثر یک‌سال پس از تخصیص بودجه مورد لزوم، بخش‌های اساسی طرح ملی تجارت الکترونیکی کشور را اجرایی نموده و طی طرح‌های زیر محقق سازد:

٤-۱- امکان‌سنجی طرح جامع تجارت الکترونیکی کشور را به انجام رسانده و برنامه درازمدت توسعه ملی تجارت الکترونیکی را برای اجرا در محدوده زمانی برنامه سوم توسعه تدوین نماید.

٤-۲- «پروژه پیشگام تجارت الکترونیکی» را به عنوان بازار نمونه داد و ستد الکترونیکی، به منظور تامین بستر ایمن لازم برای مبادلات الکترونیکی

---

۱. وزارت بازرگانی به عنوان متولی تجارت الکترونیکی در ایران، طرح‌های (نقطه تجاری ایران، ۱۳۸۳) مطالعات امکان‌سنجی تجارت الکترونیکی (متا)، ایجاد مرکز پیشگام تجارت الکترونیکی (مپتا)، ایجاد مرکز صدور گواهی دیجیتال، آموزش همگانی و ترویج استفاده از خدمات تجارت الکترونیکی، استاندارد کدینگ کالا و خدمات فعالیت‌ها، و ایجاد شبکه جامع اطلاع‌رسانی بازرگانی کشور را تبیین و تدوین نموده است.

داخلی و خارجی و ارایه خدمات جنبی مورد نیاز راه‌اندازی نماید و از اجرای پروژه‌های مشابه توسط بخش خصوصی حمایت کند.

٤-۳- مرجع صدور گواهی دیجیتال نمونه در کشور را به منظور کاربرد در حوزه تجارت الکترونیکی با لحاظ سازمان اجرایی، سخت‌افزار و نرم‌افزار لازم با استفاده از خدمات و فناوری مقبول جهانی ایجاد نماید. پس از راه‌اندازی نظام ملی مرجع صدور گواهی دیجیتال در کشور، این مرجع در چارچوب آن نظام قرار خواهد گرفت.

٤-٤- با توجه به ضرورت تقویت توان عملی داخل کشور در فناوری مربوط به گواهی دیجیتال، همزمان با اجرای بند ۳-٤ از ایجاد فناوری ملی با استفاده از نیروهای متخصص داخلی حمایت و از نتایج آن استفاده نماید.

بند ١٦. دبیرخانه شورای‌عالی اطلاع‌رسانی موظف است با مشارکت وزارتخانه‌های بازرگانی، پست و تلگراف و تلفن، اطلاعات، سازمان مدیریت و برنامه‌ریزی کشور، علوم، تحقیقات و فنّاوری، صنایع و معادن و بانک مرکزی، اقدامات لازم را برای تهیه طرح جامع حفظ ایمنی مبادلات الکترونیکی، محرمانه ماندن آمار و اطلاعات و رعایت سلامت محتوای متعلق به کاربران شبکه عمومی انتقال اطلاعات (در داخل کشور) و نظام ملی گواهی دیجیتال، به عمل آورده و برای تصویب در کمیسیون راهبردی و ارایه به شورای‌عالی اطلاع‌رسانی جهت اتخاذ تصمیم اقدام نماید.

چالش پیش روی تجارت الکترونیکی در ایران

گرچه مقدمات ورود ایران به صحنهٔ تجارت جهانی در حال فراهم‌شدن است، ولی چنانچه اصلاحات سیستم پرداخت مدنظر قرار نگیرد، فقدان سیستم‌های پرداخت الکترونیکی و به تبع آن، از دست دادن فرصت‌های بازرگانی زودگذر، کشور را در عرصهٔ جهانی به انزوا خواهد کشاند. در سیستم‌های پرداخت الکترونیکی، امنیت جایگاه ویژه‌ای دارد، که مستلزم حضور مرجع صدور گواهی است که طی برنامه سوم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران، با تدوین نظام ملی تایید هویت (CA & PKI)[۱ و ۲] و امضای دیجیتالی و نهاد مدیریت کلان آن، توسط دبیرخانه شورای عالی اطلاع‌رسانی و وزارتخانه‌ها و دستگاه‌های همکار، و

---

۱. **Public Key Infrastructure**
۲. **Certificate Authority**

طراحی، تدوین و پیاده‌سازی بانکداری الکترونیکی، توسط وزارت امور اقتصادی و بانک‌ها و شرکت‌های مخابرات، امکان‌پذیر خواهد بود (سازمان‌مدیریت‌وبرنامه‌ریزی، ۱۳۸۱؛ نصیری‌مفخّم وهمکاران، ۱۳۸۱؛ نصیری مفخّم، ۱۳۸۲).

فصل سوم:
سیستم پایاچک، مدل پیشنهادی پرداخت اینترنتی در ایران برای چک الکترونیکی

چک، یکی از اوراق تجاری است که رایج‌ترین ابزار پرداخت در ایران بوده و قائم‌مقام پول است. در حال حاضر یکی از مشکلات اقتصادی جامعه، حجم عظیم نقدینگی خارج از سیستم بانکی کشور است، که امکانات برنامه‌ریزی دقیق و اعمال سیاست‌های پولی و بانکی را محدود و در پاره‌ای موارد، غیرممکن ساخته است. لذا تلاش‌ها و برنامه‌ریزی‌ها باید با هدف جلب اطمینان و اعتماد کامل مردم، برای انجام دریافت‌ها و پرداخت‌ها در معاملات، از طریق سیستم بانکی باشد و بهترین وسیله برای اعمال چنین سیاستی حمایت کامل حقوقی و جزایی از چک است (کیانی، ۱۳۸۱؛ نبوی‌رضوی؛ ۱۳۷۰).

با آغاز تدوین قوانین تجارت الکترونیکی در کشور برای فراهم‌آوری بستر لازم جهت ورود به صحنهٔ جهانی تجارت الکترونیکی، سیستم‌های پرداخت از جمله مهمترین مواردی است که باید همراه با این حرکت، متحول شوند. از طرف دیگر، سیستم پرداختی در مورد چک سنتی به گونه‌ای است که کاستی‌های آن، مشکلاتی را درنظام اقتصادی به دنبال دارد؛ لذا در این نوشتار با توجه به نقش حساس چک در سیستم اقتصادی و لزوم مهیا شدن برای پیوستن هرچه سریع‌تر به صحنهٔ جهانی تجارت الکترونیکی، پس از مطالعهٔ انواع سیستم‌های پرداخت الکترونیکی، با توجه به ویژگی‌های ممتاز سیستم‌های از ردهٔ چک الکترونیکی که در فصل دوم اشاره شد، با مقایسه و بررسی نقاط قوت و ضعف سیستم‌های چک الکترونیکی موجود در دنیا به منظور رفع خلأهای موجود در قانون و نظام پرداخت چک، و نیز به منظور ارایه سیستمی جهت پیوستن به عرصهٔ تجارت الکترونیکی، مدلی برای یک سیستم چک الکترونیکی با توجه به وضعیت فعلی صنعت بانکداری در ایران معرفی می‌گردد.

تحلیل وضعیت جاری نظام پرداخت چک کاغذی در ایران و مشکلات ناشی از کاستی قانون چک

طبق ماده ۳۱۰ قانون تجارت جمهوری اسلامی ایران، چک نوشته‌ای است که به موجب آن، صادرکننده وجوهی را که در نزد محال علیه دارد، کلاً یا

بعضاً مسترد یا به دیگری واگذار می‌نماید. در ایران، چک نسبت به دیگر اسناد تجاری رواج بیشتری یافته است و در نتیجه از بدو تصویب قوانین مرتبط[1] مسئله‌آفرین بوده، و عمده‌ترین مشکل، مربوط به عدم پرداخت وجه آن بوده است، به طوری که با افزایش نسبت استفاده از چک، درصد جرایم مربوط به آن نیز افزایش یافته است (جدول ۳-۱).

اساساً هدف قانون‌گذار، استفاده از چک در معاملات نقدی و استفاده از سفته و برات جهت معاملات غیر نقدی است. چک، سندی تجاری است که از تضمینات محکم و قوی قانونی برخوردار است، زیرا می‌توان تحت شرایطی، صادرکنندهٔ آنرا تحت تعقیب قرار داد و حتی می‌توان برای وصول چک از طریق اجرای ثبت اقدام نمود و برای مطالبه مبلغ آن به راه‌های حقوقی متمسک شد، به طوری که مطابق ماده ۳۱٤، مقررات این قانون در مورد ضمانت صادرکننده، ظهرنویسان، اعتراض، اقامه دعوی و مفقودشدن اسناد تجاری، شامل چک نیز می‌شود. از این‌رو، مزیت چک بر سایر اسناد بهادار نظیر سفته و برات، علاوه بر قدرت نقدی چک، در صورت تخلف مجازات کیفری و جزائی صادرکننده چک می‌باشد، در حالی‌که سفته صرفاً جنبه جزائی داشته و در صورت تخلف حداکثر می‌توان اموال صادرکنندهٔ سفته را تملک و تصاحب نمود. یعنی سفته، ضمانت اجرایی دارد، درحالیکه چک از ضمانت حقوقی برخوردار است، و این پشتوانه قوی، در ماده ۱۸ قانون چک تصریح گردیده است.

از منظر علوم بانکداری، افزایش کاربرد چک در بین مردم، برابر است با هدایت پول مردم به بانک و در نتیجه افزایش سرمایه‌گذاری و این امر زمانی اتفاق خواهد افتاد که اعتماد عمومی نسبت به چک جلب شده باشد و گرایش عمومی نسبت به آن بوجود آید، ولی افزایش جرائم مربوط به آن، مانع جدی بر سر راه گسترش کاربرد چک می‌باشد (کیانی، ۱۳۸۱؛ نبوی رضوی؛ ۱۳۷۰؛ نصیری‌مفخم، ۱۳۸۲).

۱ـ چند ماده از قانون تجارت که در سال ۱۳۱۱ به تصویب رسید، به چک اختصاص یافت. ولی در سال‌های ۱۳۱۲ ، ۱۳۳۱، ۱۳۳۷، ۱۳٤٤، ۱۳۵۵، ۱۳۷۲، ۱۳۷۵، ۱۳۷٦ (دوبار)، قانون جداگانه‌ای برای چک تصویب شد و اضافاتی در مورد مقررات جزایی و کیفری و مدنی بر آن صورت گرفت. از سال ۱۳۸۲ نیز، اصلاحات قانون چک مجدداً در مجلس محترم شورای اسلامی در جریان است.

جدول ۳-۱- درصد ترکیب پول و جرائم

سال	۵۹	۶۰	۶۱	۶۲	۶۳	۶۴	۶۵	۶۶	۶۷	۶۸	۶۹	۷۰	۷۱	۷۲	۷۳	۷۴	۷۵	۷۶	۷۷	۷۸
درصد پول	۵۵/۹	۵۲	۴۷/۱	۴۹/۵	۴۴/۹	۴۴/۲	۴۵/۵	۴۴	۴۴/۴	۴۰/۶	۳۶/۸	۳۳/۶	۳۲/۷	۳۰/۵	۲۸/۶	۲۶/۱	۳/۵	۲۴/۳	۲۲/۶	۲۵/۵
درصد چک	۴۴/۱	۴۸	۵۲/۹	۵۰/۵	۵۵/۱	۵۵/۸	۵۴/۵	۵۶	۵۵/۶	۵۹/۴	۶۳/۲	۶۶/۴	۶۷/۳	۶۹/۵	۷۱/۴	۷۳/۹	۹۶/۵	۷۵/۷	۷۷/۴	۷۴/۵
درصد جرائم	-	-	-	-	-	۱	۱	۱	۲	۳	۶	۷	۸	۱۰	۱۱	۱۱	۱۲	۱۲	۱۲	۱۲/۵

منبع: کیانی (۱۳۸۱)

آمارهای مربوط به فاصله سالهای ۱۳٦٤ تا ۱۳۷۹ (جدول ۳-۱) بیان می‌کند که اگرچه میزان رشد درصد چک در حجم نقدینگی کشور، تنها ۳٤ ٪ بوده است، ولی جرائم مربوط به آن از رشد ۱۱۵۰٪ برخوردار بوده و در صورت ادامهٔ این روند، نه تنها چک، تسهیل‌کننده تجارت نخواهد بود، بلکه بر خلاف اهداف تعریف شدهٔ آن، موجب صرفه‌جویی در هزینه‌های چاپ و نشر اسکناس وتوسعه اقتصادی نیز نخواهد شد.

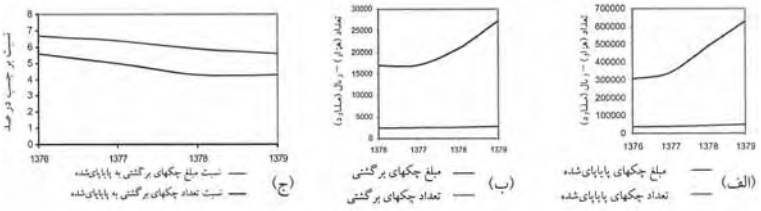
جدول ۳-۲- عملیات اتاق پایاپای چکها در فاصله سالهای ۱۳۷۶ و ۱۳۷۹

(هزار برگه – میلیارد ریال)

	(الف) چکهای پایاپای‌شده		(ب) چکهای برگشتی		نرخ الف نسبت به ب (درصد)	
	تعداد	مبلغ	تعداد	مبلغ	تعداد	مبلغ
۱۳۷۶	۳۶,۹۳۲	۳۰۵,۸۸۳	۲,۴۵۹	۱۷,۰۱۸	۶/۷	۵/۶
۱۳۷۷	۳۹,۹۶۵	۳۴۴,۰۱۴	۲,۵۷۵	۱۷,۰۴۲	۶/۴	۵/۰
۱۳۷۸	۴۴,۷۰۵	۴۸۸,۹۲۸	۲,۶۳۲	۲۰,۸۵۸	۵/۹	۴/۳
۱۳۷۹	۵۰,۱۹۲	۶۳۰,۸۴۰	۲,۸۱۷	۲۷,۳۱۵	۵/۶	۴/۳

منبع: بانک مرکزی جمهوری اسلامی ایران (۱۳۸۰)

شکل ۳-۱-عملیات اتاق پایاپای چکها در فاصله سالهای ۱۳۷۶ و ۱۳۷۹
(الف) چکهای پایاپای‌شده (ب) چکهای برگشتی (ج) نسبت این دو



منبع: نصیری‌مفخّم (۱۳۸۲)

همچنین آمارها نشان می‌دهد که ۳۵ ٪ از مجرمان و ٤٧٪ از قضات کشور، وضعیت نامناسب اقتصادی (نوسانات شدید اقتصادی نظیر افزایش شدید قیمت‌ها، از دست دادن شغل، کاهش ارزش پول ملی، تصمیمات ضد و نقیض متولیان امور اقتصادی) را مهم‌ترین عامل صدور چک بی‌محل می‌دانند و از طرفی ۳۲٪ از قضات، عملکرد نامناسب بانک‌ها در تحویل دسته چک را به عنوان عامل بعدی مورد شناسایی قرار داده‌اند. وضعیت نامناسب اقتصادی را می‌توان در نبود تحرک کافی بانک‌ها و عدم ابزارهای مناسب پولی و بانکی نیز برشمرد (کیانی، ۱۳۸۱؛ نصیری‌مفخّم، ۱۳۸۲). آمار عملیات اتاق پایاپای چک‌ها در فاصله سال‌های ۱۳۷٦ تا ۱۳۷۹ (مطابق جدول ۳-۲ و شکل ۳-۱) نشان می‌دهد که بر اساس سیاست‌های به کار گرفته شده، رشد چک‌های برگشتی نسبت به رشد چک‌های پایاپای‌شده کمتر بوده است، بطوریکه نسبت این دو، روند کاهشی را طی کرده است. ولی آنچه مسلم است آن است که با گران‌ترشدن کالاها، متوسط مبلغ هر چک، از ۸/۳ میلیون ریال به ۱۲/۷ میلیون ریال رسیده است، که این موضوع نشانگر نرخ تورم است. ولی رشد تعداد چک‌ها، بیانگر افزایش فعالیت‌های اقتصادی طی این مدت است (نصیری‌مفخّم، ۱۳۸۲).

از طرف دیگر، سیستم پرداختی در مورد چک سنتی به گونه‌ای است که کاستی‌های آن، مشکلاتی را درنظام اقتصادی به دنبال دارد. در مورد قانون چک، اخیراً بحث‌هایی از طرف حقوقدانان و صاحب‌نظران مطرح شده است و ایراداتی را بر آن بیان نموده‌اند. از جملهٔ این موارد در مباحث اصلاح قانون چک، ضرورت ردپای چک است (بانک ملت، ۱۳۸۱؛ مهدوی، ۱۳۸۱-۱-۲؛ وزارت کار و امور اجتماعی، ۱۳۸۱؛ نصیری‌مفخّم، ۱۳۸۲). مشکلات و نیازهایی که در این رابطه ذکر شده، به قرار زیر است (مهدوی، ۱۳۸۱-۲؛ نصیری‌مفخّم، ۱۳۸۲):

(الف) انتقال پول به شخص ثالث از طریق «صدور چک در وجه حامل» بدون ایجاد ردپای قانونی و اسناد و مدارک معتبر جهت اثبات رابطهٔ مالی بین صادرکننده و وصول‌کنندهٔ چک و بدون ثبت در سیستم‌های بانکی صورت می‌گیرد.

(ب) لازم است امضای ظهرنویس توسط یکی از بانک‌های رسمی یا یکی از دفاتر اسناد رسمی مورد گواهی قرار گیرد، تا از یک طرف از انتقال پول از طریق صدور چک به نام مستعار و یا ظهرنویسی جعلی جلوگیری شود و از طرف دیگر، گیرندگان چک به واریز چک‌های وصولی به حساب جاری خود و پرداخت دیون خود از طریق صدور چک شخصی ـ از این طریق، ایجاد ردپاـ تشویق شوند.

(ج) بانک‌ها به ارسال اصل چک‌های کارسازی شده یا رونوشت پشت و روی برابر اصل شدهٔ چک‌های کارسازی شده برای صاحب حساب، هم‌زمان با ارسال صورت‌حساب به سپرده‌گذار، مکلّف گردند.

(د) اهتمام و مساعی دولت در جهت حفظ حقوق و منافع گیرندگان چک، به جای زندانی‌کردن صادرکنندگان چک پس از معامله، باید جهت آگاهی و مطلع نمودن گیرندگان چک از میزان اعتبار صادرکنندگان چک، قبل از انجام معامله باشد.

(هـ) در خصوص تجهیز دریافت‌کنندگان چک به اطلاعات کافی در خصوص اعتبار صادرکنندگان چک، پیشنهاد شده است که مؤسسات خصوصی تأییدکنندهٔ چک تأسیس گردد و بانک‌ها مکلف به جمع‌آوری اطلاعات مربوط به تعهدات آشکار اشخاص حقیقی و حقوقی شوند.

برآورده شدن این موارد، منتج به افزایش درآمد مالیاتی دولت، کاهش تعداد مؤدیان مالیاتی فرار از مالیات، کاهش امکان سوءاستفادهٔ مأمورین دولتی و اخذ مالیات غیرموجه و نهایتاً کاهش فعل و انفعالات مالی و معاملات غیرمجاز خواهد شد. هرگاه ردپای پول وجود داشته باشد، دولت می‌تواند بدون اجحاف، حق قانونی خود را وصول نماید.

بدین ترتیب مشاهده می‌شود که چک‌های الکترونیکی راه حل این مشکلات هستند. در یک سیستم چک الکترونیکی، دریافت‌کننده، چکها را به بانک خود ارایه داده و درخواست‌های پایاپای چک توسط بانک دریافت‌کننده، تقریباً همان

موقعِ صدور چک می‌تواند برای بانک پرداخت‌کننده اجرا شود. لذا دیگر صدور چکِ با ماندهٔ بدهکاری[۱] امکان ندارد، و هر چند این موضوع از دیدگاه جریانات نقدی پرداخت‌کنندگان خبر خوبی نیست، ولی بدین طریق تحقق مادهٔ ۳۱۱ و ۳۱۳ قانون تجارت در مورد چک امکان‌پذیر می‌گردد و موردی نیز برای جرائم مطرح در مادهٔ ۱۳ قانون چک نخواهد بود.

با توجه به ویژگی‌های امضاهای دیجیتالی و ویژگی‌های چک الکترونیکی، به دلیل ثبت اطلاعات چک الکترونیکی در تمام محل‌های صدور یا وصول، مشکل (الف) منتفی است. گواهی‌های دیجیتالیِ کلید عمومی امضا، مورد (ب) را برآورده می‌سازند. با توجه به مواردی که برایِ (الف) ذکر گردید، مورد (ج) نیز برآورده می‌شود. با بلادرنگ شدن ارتباطات طرفین با یکدیگر و با بانک‌هایشان، مورد (د) نیز تأمین می‌گردد. در مورد (هـ) مشاهده می‌شود که به خوبی، نیاز به حضور مرجع صدور گواهی احساس شده است و گواهی‌های دیجیتالی صادره از سوی مرجع صدور گواهی دیجیتالی، به این نیاز پاسخ می‌گویند. گواهی‌های دیجیتالی همهٔ طرف‌ها، همواره همراه چک الکترونیکی هستند و در هرکدام از مراحل چرخهٔ زندگی چک، بررسی‌های لازم قابل انجام هستند. جدول(۳-۳) خطراتی را که برای برهم‌کنش‌کنندگان در یک تراکنش چک سنتی ممکن است مطرح باشد و با سیستم چک الکترونیکی برطرف خواهد شد، ارایه می‌دهد.

---

۱. **overdraft**

با توجه به جایگاه ویژه و مزایای چک در نظام بانکی و مشکلاتی که این ابزار با آن مواجه است، لازم است با هدف «فائق آمدن بر مشکلات چک سنتی و ورود به عرصهٔ تجارت الکترونیکی»، «افزایش سرعت عملیات بانکی مرتبط با چک»، «کاهش هزینه‌های بایگانی و نگهداری اسناد مرتبط با چک»، «کاهش هزینه‌های اجتماعی ناشی از صدور چک‌های بلامحل»، «بکارگیری

پیشرفت‌های فناوری تجهیزات کامپیوتری» و «همسویی با استقبال عمومی از پرداخت‌های الکترونیکی در سطح جوامع» (کیانی، ۱۳۸۱؛ نصیری‌مفخّم، ۱۳۸۲؛ نصیری‌مفخّم و همکاران، ۱۳۸۱)، سیستمی برای چک الکترونیکی در ایران

طراحی و پیاده‌سازی گردد. لذا به منظور رفع خلأهای موجود در قانون و نظام پرداخت چک و ورود به عرصهٔ تجارت الکترونیکی، در بخش بعد مدلی برای سیستم چک الکترونیکی (دیجیتالی)، به عنوان ابزار و روش پرداخت اینترنتی در ایران، تحلیل و طراحی می‌گردد.

جدول ۳-۳- حذف مخاطرات برای برهمکنش کنندگان در سیستم چک الکترونیکی

شرح ریسک	طرفی که در معرض بیشترین ضرر است	تأثیر چک الکترونیکی
چکهای دزدیده شده	بانک و شخص دریافت کننده اولیه	کاهش از طریق سخت‌افزار با حفاظت PIN
صدور غیر قانونی	پرداخت کننده	کاهش از طریق انتساب شخصی نشانه‌های امضا و همچنین امضای دوگانه یا دویل
جعل (forgery)	دریافت کننده و بانک پرداخت کننده	حذف مجازی از طریق امضای دیجیتالی، تصدیق خودکار و کلیدهای امضای سخت‌افزاری با حفاظت PIN
جعل، هنگامی که از امضای جوهری فاکسی‌مایل روی حساب استفاده می‌شود	دریافت کننده، دارنده حساب	حذف شده است
نسخه برداری (المثنی) (counterfeiting)	دریافت کننده، بانک صاحب پس‌انداز بانک پرداخت کننده	کاهش از طریق عملیات آشکارسازی نسخه‌برداری دقیق، استفاده از کلید عمومی دریافت کننده علاوه بر نام
تقلب و جعل (duplication)	بانک پرداخت کننده، دریافت کننده	از طریق امضای دیجیتالی تقریباً حذف شده است. تأیید خودکار و کلید امضای سخت‌افزاری با حفاظت PIN
بسرات عندالمطالبه (demand) امضا نشدهٔ تقلبی	دریافت کننده، بانک صاحب پس‌انداز بانک پرداخت کننده	حذف شده است
تغییر نام دریافت کننده	بانک صاحب پس‌انداز*، دریافت کننده تقلبی، پرداخت کننده	بطور مؤثر حذف شده است
تغییر مقدار (بدون پرداخت مثبت)	بانک صاحب پس‌انداز*، دریافت کننده	بطور مؤثر حذف شده است
تغییر مقدار (با پرداخت مثبت)	بانک صاحب پس‌انداز*، دریافت کننده	بطور مؤثر حذف شده است
اشتباه در رمزگشایی مقدار	بانک صاحب پس‌انداز، دریافت کننده خطای کوچک هنگام پردازش توسط بانک	حذف شده است
عدم موجودی کافی، بسته بودن حساب	دریافت کننده**	کاهش از طریق زمان تسویه سریعتر
قطع پرداخت	دریافت کننده**	کاهش از طریق زمان تسویه سریعتر
چک کشیده شده روی بانک یا حسابی که وجود ندارد	دریافت کننده	حذف از طریق مجوز حساب دیجیتالی که توسط بانک به صاحب حساب داده می‌شود

* فرض می‌شود که واگذار کننده، پول را اخذ می‌کند (depositing bank)

** حفاظت از خود با تأخیر حمل کالاها، گواهی لازم یا چکهای صندوقداران، یا با فرآیندهای تسویه بلادرنگ

منبع: گلیناس (۲۰۰۱)

سیستم *پایاچک*، مدل پیشنهادی پرداخت اینترنتی در ایران برای چک الکترونیکی

از میان سیستم‌های طراحی شده یا موجود چک الکترونیکی در دنیا که در فصل دوم از نظر گذراندیم، تنها دو سیستم چک الکترونیکی FSTC[1] و MANDATE[2] به سطح پروتوتایپ عملی یا آزمایشی رسیده‌اند. از آنجا که ایده و مفهوم چک الکترونیکی (در تطابق با قانون چک و قابلیت فراتر از نسخهٔ کاغذی آن) توسط کنسرسیوم FSTC پایه‌گذاری گردیده، و سایر سیستم‌های MANDATE و e-Check[3] نیز از بدنهٔ قوی مدل آن الهام گرفته‌اند، ما نیز در این تحقیق با تحلیل نیازهای پوشش داده نشده در قانون چک در رسیدن به مدل عملی، ضمن وقوف به ویژگی‌های شایستهٔ FSTC eCheck، بی‌تأثیر از آن نبودیم.

در این بخش مدل جدیدی ارایه می‌شود[4]، که ضمن برخورداری از سهولت پرداخت چک الکترونیکی روی اینترنت و امکان بررسی سریع موجود بودن وجه، این امکان را فراهم می‌سازد که مشتریان بر اساس درجه‌ای از اعتبارشان، از طرف شرکت ثالثی موسوم به مؤسسهٔ عامل[5] (که نقش آن در دنیای فیزیکی، خریدن چک‌های برگشتی به کسری از قیمت است)[6]، چک برگشتی آنها پرداخت شود، و درعوض متحمل درصد هزینهٔ بیشتری برای پردازش چک‌های آتی‌شان باشند. چنانچه شرکت ثالث، چک برگشتی آنها را پرداخت نکند، در اینصورت، برگشتی بودن چک به بانک مشتری و نهایتاً به بانک تاجر و شخص تاجر و خود مشتری اعلام می‌گردد. بدین طریق ضمن حفظ اسرار مالی مشتریان، امکان پرداخت شدن چک‌های مشتریان خوش اعتبار که به طور ناخواسته و به دلیل اشتباه برگشت خورده است، فراهم می‌گردد. به منظور پایاپای نقدی بانک‌های مشتری و تاجر، از «شتاب»[7] استفاده می‌شود. از طرفی، با محقق شدن سیستم تسویه ناخالص بلادرنگ (RTGS[8]) (هنکوک، ۱۹۹۸؛ خیائونارانگ، ۲۰۰۰؛ کمیته تحقیقاتی کاربرانی ایرانی سوئیفت، ۱۳۸۲)، بانک‌هایی که سپرده‌شان در بانک مرکزی، کمتر

۱ـ بخش ۲-۳-۱ را ببینید.

۲ـ بخش ۲-۳-۲ را ببینید.

۳ـ بخش ۲-۳-٤ را ببینید.

٤ـ دو راهکار دیگر نیز در (نصیری‌مفخّم، ۱۳۸۲، فصل چهارم، بخش ٤-۳-۱ و ٤-۳-۲)، یکی تقریباً مشابه e-Check هندوستان و دیگری با تمرکز بر قابلیت‌های شبکهٔ سوئیفت پیشنهاد شده که این مدل سوم، مشکلات آن دو راهکار پیشنهادی دیگر را نیز برطرف می‌نماید.

۵ . Factor Company

٦ـ در ماده ۲۳۹ قانون تجارت، می‌توان به نوعی نقش شخص ثالث یا شرخر را مشاهده کرد: هرگاه براتی نکول شد و اعتراض به عمل آمد شخص ثالثی می‌تواند آن را به نام برات‌دهنده یا یکی از ظهرنویس‌ها قبول کند- قبولی شخص ثالث باید در اعتراض نامه قید شود و به امضا او برسد.

۷ـ شبکهٔ تبادل اطلاعات بین بانکی - فصل دوم، بخش ۲-۵-۲.

۸. Real-Time Gross Settlement

از مبلغ چک وارده برای تسویه باشد، قادر به تسویهٔ چک مشتری خود نخواهند بود، و از این‌رو بانک‌ها نیز برای پائین نگه داشتن درصد چک‌های برگشتی خود، نسبت به حفظ سپردهٔ مناسب در بانک مرکزی از طریق مدیریت نقدینگی[۱] مبادرت خواهند کرد.

براساس سرنام عبارت «پـرداخت ایـنترنتی ایران برای چک الکترونیکی» که معرف ویژگی این سیستم است، این سیستم را ***پایاچک*** و به انگلیسی، *iPay-eCheck*[۲] می‌نامیم.

سناریوهای پردازش پایاچک

در فصل دوم، بخش ۲-۲، با سناریوهای پردازش چک الکترونیکی که FSTC بیان نموده، آشنا شدیم. اگر به عقب برگردیم و به شکل ۲-۵ مراجعه کنیم، بر اساس آنچه که در خصوص مزایا و ویژگی‌های قانونی چک صحبت کردیم، واضح است که مدل ۲-۵-(د) که همان حوالهٔ الکترونیکی است، یک روش پیش‌پرداخت است و چون قانونی در پشت سر حواله نیست، فروشنده صرفاً باید به طریقی online (اعلام بانک) از پرداخت از طرف خریدار مطمئن شود، در حالی‌که در مدل‌های۲-۵-(الف) و ۲-۵-(ب)، به حکمَ سند امضا شدهٔ چک که در دست فروشنده است، خریدار مکلف به پرداخت مبلغ به دارندهٔ سند چک می‌باشد. همچنین در مدل ۲-۵-(ج) که گونه‌ای از مدل ۲-۵-(الف) است، خریدار مکلف به پرداخت مبلغ به بانک فروشنده است و بانک فروشنده سند چک را در اختیار دارد.

از طرفی در مدل سیستم *پایاچک*، دو گونه خدمات چک الکترونیکی از سوی بانک‌ها، یکی خدمات به دارندگان حساب‌های جاری و دیگری، خدمات به دارندگان حساب‌های پس‌انداز، در نظر می‌گیریم. در نوع اول، دارندهٔ دسته چک الکترونیکی هم قادر به صدور و امضای چک برای ارسال به فروشنده است، و هم قادر است چک‌های الکترونیکی وارده از طرف سایرین را امضا کرده و به این حساب خود واگذار نماید. در نوع دوم، صاحب حساب، صرفاً قادر به امضا کردن چک‌های الکترونیکی وارده و واگذاری به حساب خود است، ولی امکان صدور چک الکترونیکی را ندارد. پیشنهاد می‌گردد که حساب جاری مذکور، به صورت دو منظوره باشد تا صاحبان حساب به جهت سودی که از طرف بانک به آن تعلق می‌گیرد، موجودی مناسب و کافی در آن نگه دارند.

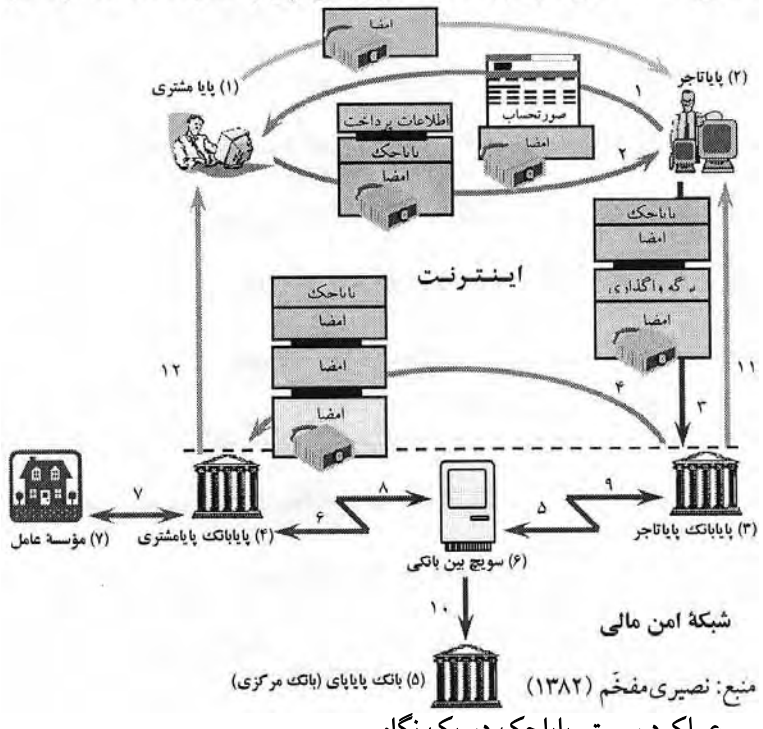
---

۱. **Liquidity management**

۲. **iranian Internet Payment System for Electronic Check**

چون در این شبکه افرادی قادر به استفاده از چک الکترونیکی هستند که از بانک‌های خود، کلیدهای امضا و گواهی دریافت کرده باشند، لذا حتی برای امضا و واگذاری چک دریافتی نیز استفاده از امضاها و ارایه گواهی ضروری است. از اینرو دیگر سناریوی مدل ۲-۵-(ب) مطرح نیست و بانک شخص فروشنده قادر به پذیرش چک است و نیازی نیست که فروشنده، چک را به بانک مشتری واگذار کند. بنابراین فقط مدل (الف) را در نظر گرفتیم و مدل پیشنهادی ما بر اساس مدل ۲-۵-(الف)، یعنی مدل «واگذاری و پایاپای» و نیز با پوشش دادن چک‌های تضمین شده است. شکل ۳-۲ نمای اولیهٔ مدل سیستم *پایاچک* را نشان می‌دهد.

شکل ۳-۲- مدل سیستم تمام الکترونیکی *پایاچک* (iPay-eCheck)



منبع: نصیری‌مفخّم (۱۳۸۲)

عملکرد سیستم پایاچک در یک نگاه

در مدل سیستم تمام الکترونیکی پایا چک با بهره‌گیری از نقش سویچ بین بانکی «شتاب»، با ترجمهٔ پیام‌های پرداخت واصله از اینترنت به دروازه‌های

پایابانک‌ها[1] به صورت پیام‌های مطابق استاندارد استفاده شده در شتاب، با امکان استفاده از مکانیزم پایاپای، کل چرخه را برای پرداخت‌های ریالی، مکانیزه می‌کنیم. قالب پیام‌های شتاب مطابق استاندارد ISO ۸۵۸۳ [2] است. در نظر است، برای پرداخت‌های ارزی نیز، برای بهره‌گیری از «سوئیفت»، پیام به فیلدهای مورد نیاز در پیامهای سوئیفتی مربوطه ترجمه گردد. بدین منظور دو مترجم دوسویه در هر دروازه لازم است (یکی برای ترجمه به پیامهای «شتاب» و بالعکس، و دیگری برای ترجمه به پیامهای «سوئیفت» و بالعکس).

ذکر این مطلب نیز لازم است که با توجه به ویژگی‌های مناسب کارت هوشمند برای سطح امنیت مناسب در کاربرد عملی، این مدل بر اساس کارت هوشمند خواهد بود، چراکه در چند سال آتی، دستگاه‌های خوانندهٔ کارت‌های هوشمند روی PCها و ایستگاه‌های کاری به وفور موجود خواهند بود، و لذا هر کاربری می‌تواند بدون نیاز به سخت افزارهای پرهزینهٔ کارت خوان، از مزایای کارت هوشمند برخوردار شود. ولی از آنجایی که در این تحقیق از نظر محدودیت زمانی و هزینه، استفاده از این فنّاوری ممکن نبود، در سطح شبیه‌سازی و پروتایپی از این مدل پیشنهادی که در فصل چهارم می‌آید، از فلاپی دیسک برای ذخیرهٔ کلیدهای امضا و گواهی، و اطلاعات دسته چک استفاده گردید.

در این مدل، ویژگی دیگری نیز افزون بر ویژگی‌هایی که MANDATE و e-Check به منظور صدور و تجدید دسته چک دارند، در نظر می‌گیریم. از آنجایی که وقتی اعتبار کلید و گواهی کارت سربیاید، دیگر امکان استفاده از آن برای ارسال محرمانه و امن پیام نیست، لذا علاوه بر «زوج کلید امضا»، زوج کلیدی تحت عنوان «کلید کاربری» (در قیاس با شماره مشتری در حساب‌های بانکی) تعریف می‌کنیم، به طوریکه کاربر با استفاده از این زوج کلید برای ارسال پیام درخواست تجدید گواهی و اطلاعات دسته چک الکترونیکی جدید اقدام می‌کند، و با پیام دریافتی از بانک، دسته‌چک جدید روی کارت قبلی بارگذاری می‌شود. برای گواهی «زوج کلید کاربری» مدت اعتبار بیشتری نسبت به «زوج کلید امضا» در نظر گرفته می‌شود.

یکی از علایق مشتریان به استفاده از چک، شناوری آن است که با بررسی و اِعمال بلادرنگ پرداخت از حساب آنها، مدت آن کوتاه می‌گردد، و در مواردی

۱ـ بخش ۳-۲-۳ (تعریف پایابانک) و بخش ۳-۲-٤ را ببینید.

۲. **AZS Services,2002’ Triversity product Development,2003؛ Trasted Security Solutions , 2000؛**

امکان برگشت خوردن چک به دلیل محاسبهٔ اشتباه زمان واریز وجه به حساب پیش بیاید، مؤلفه (یا به عبارتی مؤسسه) دیگری در نظر گرفته‌ایم، که مشتریانی که مایل به استفاده از خدمات حمایتی آن باشند، می‌توانند با ارایه مدارک لازم در آنجا ثبت نام کنند. این مرکز، مؤسسه‌ای موثق و با مجوز از بانک مرکزی جمهوری اسلامی ایران است. از این پس، این مؤسسه صرفاً از طریق بانک مشتری، برهم‌کنش‌هایی را برای پوشش دادن به چک‌های برگشتی در حد اعتماد مؤسسه انجام می‌دهد. از آنجا که برهم‌کنش با مؤسسهٔ عامل، تنها در موارد پرداخت نشدن چک‌های مشتریان و نه در تمام فرایندها صورت می‌گیرد، لذا ضمن بهره‌گیری از مزایای الکترونیکی پرداخت، همچون صحت، سرعت و سهولت، در موارد برگشت چک‌ها نیز فرایند رسیدگی و پرداخت به صورت الکترونیکی، سریع، امن و خودکار انجام می‌شود و سرباری بر روند دیگر تراکنش‌های عادی سیستم اعمال نمی‌کند.

سیستم پایاچک در سمت هر کدام از بانک‌های مشتری و تاجر، یک دروازهٔ (حداقل) سه طرفه است. این دروازه، از یک سو با اینترنت، از سوی دیگر با شبکهٔ سیستم بانکی آن بانک و شعب مربوطه، و از دیگر سو، با شبکهٔ بین بانکی برهم‌کنش دارد. در صورت پرداختهای ارزی، اتصال با شبکهٔ بین‌بانکی بین‌المللی (سوئیفت) نیز لازم است. ساختار مورد استفاده برای پیام‌ها، XML در نظر گرفته می‌شود که باید به قالب‌های بین بانکی لازم ترجمه گردد. این دروازه، با سرور صدور امضا و گواهی دیجیتالی پایابانک نیز در ارتباط است.

ضمناً کاربران از طریق یک سیستم پیام‌رسانی که به صورت «ذخیره و ارسال»[1] هم به حالت off-line و هم On-line[2]، پیام‌های مرتبط با چک و پرداخت را در صندوق پستی خاص در آن سرور پیام‌رسانی به صورت خودکار می‌تواند پردازش کند، از سیستم استفاده می‌کنند. ساختار واسط این صندوق پستی الکترونیکی به گونه‌ای است که اطلاعات فیلدهای پیام‌های ورودی و خروجی آن (حاصل از پردازش خودکار سند XML) به صورت فیلدهایی از یک جدول، داده‌های مربوط به چک‌های پرداختی یا دریافتی را به کاربر نشان می‌دهد و او می‌تواند از گزینه‌های در دسترس، عمل مورد نظر را روی آن قلم انجام دهد. بخش اصلی سیستم *پایاچک*، در سمت بانک‌ها است که کاربران از

---

۱. store & forward (مشابه روش مورد استفاده در سوئیفت)

۲ـ مشابه Yahoo! Mail و Yahoo! Messenger همراه باهم.

طریق ورود به آن، اقدام به پرداخت با *پایاچک* برای خریدهای خود می‌کنند. برای شرح این مراحل، لازم است ابتدا چند تعریف ارایه کنیم.

برهم‌کنش موجودیت‌ها در سیستم *پایاچک*

در یک فرایند معامله توسط *پایاچک*، همانگونه که در شکل۳-۲ نشان داده شده است، پایامشتری، پایاتاجر، پایابانک پایاتاجر، پایابانک پایامشتری، بانک پایاپای، سویچ پایاپای بین بانکی، و مؤسسهٔ عامل حضور دارند. ویژگی‌های هر یک از این موجودیت‌ها را طی تعاریفی، در زیر بیان می‌کنیم (نصیری‌مفخّم، ۱۳۸۲).

***پایابانک* (بانک ارایه دهندهٔ خدمات *پایاچک*):** بانکی می‌تواند ارایه‌دهندهٔ خدمات *پایاچک* باشد که: ۱) سیستم هستهٔ بانکی آن به صورت شبکه‌ای با ارتباط پیوسته با شعب آن بانک باشد، ۲) مجوز ارایه این خدمات را با دریافت امضا و گواهی دیجیتالی از بانک مرکزی جمهوری اسلامی ایران کسب کرده باشد (بانک مرکزی، امضا و گواهی دیجیتالی خود را از مرجع صدور گواهی جمهوری اسلامی ایران کسب کرده است)[1]، ۳) به سویچ پایاپای بین بانکی کشور متصل باشد، و ٤) مجهز به دروازهٔ *پایاچک* باشد (این دروازه از یک سو با اینترنت، از یک سو با سیستم هستهٔ بانکی، از سوی دیگر با سروری که وظیفهٔ صدور کارت امضا و گواهی دیجیتالی و *دسته‌چک‌پایا* و پردازش *پایاچک*‌های واصله را برای مشتریان خود بر عهده دارد، و از دیگر سو با سویچ بین بانکی کشور اتصال دارد). چنین بانکی را *پایابانک* می‌نامیم. موجودیت‌های (۳) و (٤) در شکل ۳-۲، به ترتیب *پایابانک* پایاتاجر و *پایابانک* پایامشتری هستند.

***پایاچک*:** مطابقَ مورد ۹ قانون چَک الکترونیکی که در راستای این تحقیق پیشنهاد شد[2]، چک الکترونیکی نوشته‌ای الکترونیکی است که به موجب آن، صادرکننده وجوهی را که در نزد محال علیه دارد، کلا یا بعضاً مسترد یا به دیگری واگذار می‌نماید. در تبصرهٔ این ماده، آمده است که صادرکنندهٔ پایاچک کسی است که مجوز صدور پایاچک روی حساب جاری در پایابانکی که این خدمات را ارایه می‌دهد داشته باشد (دسته چک‌پایا). همچنین دریافت‌کنندهٔ پایاچک نیز به کسی اطلاق می‌شود که مجوز وصول پایاچک روی یک حساب در پایابانکی که این خدمات را ارایه می‌دهد، داشته باشد (کارت امضای پایا). صادرکننده و دریافت‌کننده، با امضاهای دیجیتالی و گواهی امضای دیجیتالی دریافتی از پایابانک خود، مجوز استفاده از خدمات پایاچک را دریافت می‌کنند. پایابانک‌ها نیز امضای

۱ـ بخش ۳-۲-۵ را ببینید.

۲ـ موارد پیشنهادی برای قانون چک الکترونیکی در پیوست دوم از (نصیری‌مفخّم، ۱۳۸۲) آمده است.

دیجیتالی و گواهی دیجیتالی امضای خود را از بانک مرکزی (و آن‌هم به نوبه خود از مرجع صدور گواهی ایران) دریافت کرده‌اند. *پایاچک*، یک چنین چک الکترونیکی است و ساختار آن در بخش ۳-۲-٦ به تفصیل تشریح گردیده است.

دسته‌چک‌پایا/کارت امضای پایا: یک *دسته‌چک‌پایا*، وسیله‌ای است که دربردارندهٔ کلیدها و گواهی امضا و اطلاعات مرتبط با دارندهٔ حساب و *پایابانک* مربوطه و روتین‌هایی برای کنترل دسترسی و استفاده از امضاها و اطلاعات حساب و صدور/واگذاری *پایاچک*‌های یکتا است.

پایامشتری، پایاتاجر: کلیهٔ دارندگان حساب در یک *پایابانک* می‌توانند *پایاچک* دریافتی از پایاکاربران هر شعبه‌ای از هر پایابانکی را به حساب خود واگذار کنند، ولی صرفاً دارندگان حساب‌های جاری *پایابانک* با دریافت *دسته‌چک‌پایا*، امکان استفاده از خدمات صدور *پایاچک* را برای پرداخت‌های اینترنتی خود دارند. دارندگان حسابهای نوع اول را *پایاتاجر*، و دارندگان حساب‌های نوع دوم را *پایامشتری* می‌نامیم. سایت اینترنتی بنگاه تجاری یک *پایاتاجر* را یک *پایابنگاه* می‌نامیم. پایامشتری و پایاتاجر با امضاهای دیجیتالی دریافتی از پایابانک خود، مجوز استفاده از خدمات پایاچک را دریافت می‌کنند. یک *پایامشتری* می‌تواند از روی یک *پایابنگاه* با *پایاچک* خرید نماید. در شکل ۳-۲، موجودیت (۱) *پایامشتری* و موجودیت (۲) *پایاتاجر* است.

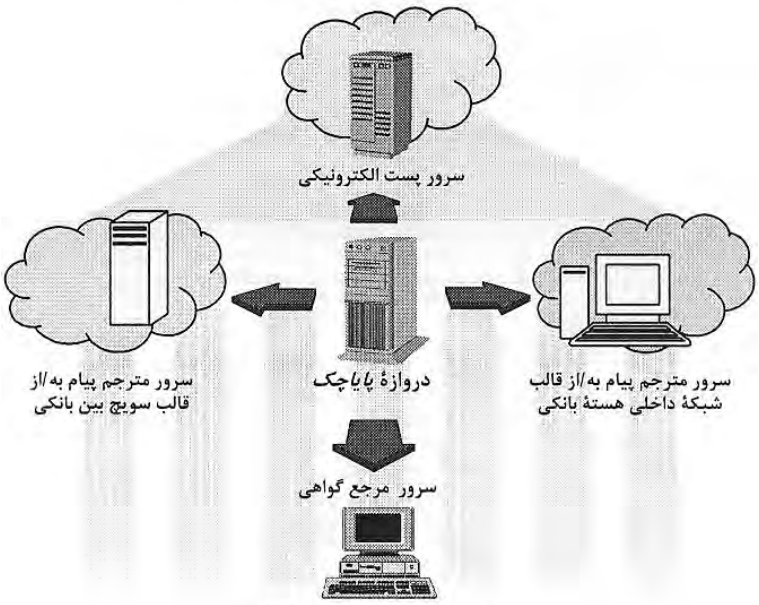
بانک پایاپای: جهت عملیات بین بانکی، هر یک از پایابانک‌ها حسابی نزد بانک پایاپای (بانک مرکزی) دارند. وقتی یک پایابانک، پایاچکی عهدهٔ پایابانک دیگری از پایاکاربر دریافت کند که باید پایاپای گردد، آن مبلغ باید در حساب‌های دو پایابانک نزد موجودیت (۵) اعمال شود.

سویچ بین بانکی: این موجودیت که وظیفهٔ مبادلهٔ اطلاعات بین بانکی را دارد، اطلاعات مورد نیاز برای پایاپای را به پایابانک مربوطه رسانده و عملیات را ثبت می‌کند. بدهکاری و بستانکاری نظیر این عملیات، روی حساب‌های پایابانک‌های مربوطه نزد بانک پایاپای اعمال می‌شود. موجودیت (٦) در شکل ۳-۲، نشانگر این سویچ است.

مؤسسهٔ عامل: *پایامشتری* می‌تواند در مؤسسهٔ عامل، ثبت نام و برحسب ضوابط آن (سپردن وثیقه،...)، اعتباری برای خود منظور نماید. در نگاه اول، مؤسسهٔ عامل می‌تواند همچون بانک کارگشایی باشد؛ حسابی نزد بانک مرکزی داشته باشد، و همچون سایر *پایابانک*‌ها از طریق سویچ پایاپای با دیگر *پایابانک*‌ها پایاپای نماید. ولی از آنجا که این مؤسسه مطابق قوانین حاکم بر شبکه‌های بین

بانکی، ماهیتاً بانک نیست، لذا مؤسسهٔ عامل بایستی یک حساب نزد هر *پایابانک* ـ نه در همه شعب ـ داشته باشد. چنانچه براثر اشتباهات و تأخیر در موجود نگه داشتن وجه در حساب، *پایاچک* *پایامشتری* وصول نشود، آن مؤسسه از طرف *پایامشتری*، وجه *پایاچک* را از حساب خود در آن *پایابانک* می‌پردازد. *پایامشتری* بابت دریافت این گونه خدمات، باید سالانه هزینه‌ای متحمل شود. این موجودیت تحت شماره (۷) در شکل ۳-۲ نشان داده شده است.

شکل ۳-۳ نمای یک پایابانک



منبع: نصیری‌مفخّم (۱۳۸۲)

دروازهٔ پایاچک در یک پایابانک

در بخش ۳-۲-۲ گفته شد که بخش اصلی سیستم *پایاچک*، در سمت *پایابانک*‌ها است که *پایامشتری*‌ها از طریق ورود به آن، اقدام به صدور *پایاچک* برای پرداخت خریدهای خود می‌کنند. *پایاتاجرها* نیز با ورود به سیستم *پایابانک* خود، درخواست *واگذاری* *پایاچک*‌های واصله را می‌کنند. شکل ۳-۳

نمای یک *پایابانک* را که در شکل ۳-۲ به صورت کلی نشان داده شده بود، به تصویر می‌کشد. در *پایابانک پایامشتری*، ارتباطی با (شبکهٔ) مؤسسهٔ عامل برای بررسی اعتبار *پایاچک*‌های برگشتی *پایامشتری*‌ها نیز برقرار است.

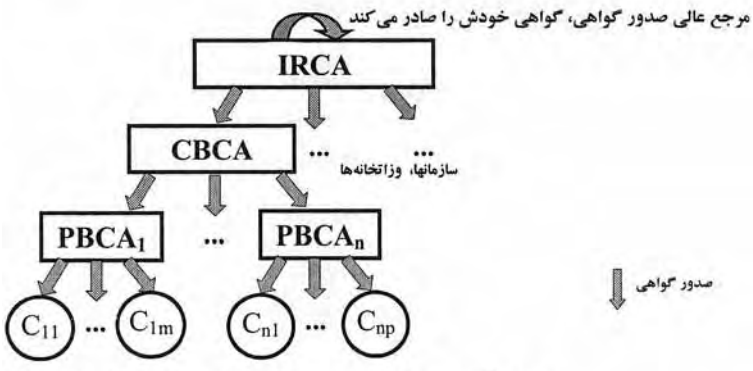
زنجیرهٔ اعتماد در سیستم پایاچک

چنانچه گفته شد، برای اینکه سیستم مورد اعتماد باشد، هر کدام از پایامشتری‌ها، پایاتاجران و پایابانک‌ها، دارای گواهی دیجیتالی و کلیدهای عمومی و خصوصی امضا هستند. پایابانک‌ها به عنوان مرجع صدور گواهی عمل نموده و برای پایاکاربران، گواهی امضای دیجیتالی صادر می‌نمایند. با توجه به مفاهیمی که در تعاریف فوق ذکر گردید، *پایابانک*‌ها در این سیستم براساس گواهی امضایی که از بانک مرکزی کسب نموده‌اند، صحت هویت یکدیگر را شناسایی کرده و می‌توانند *پایاچک*‌های یکدیگر را مبادله و پایاپای نمایند. این فرایند هویت‌شناسی دو مزیت دارد: احرازکنندهٔ صحت هویت، فقط نیاز به دانستن کلید عمومی گواهی سطح بالاتر دارد، ولی پرداخت‌کننده و دریافت‌کننده لازم نیست کلیدهای عمومی یکدیگر را بدانند. پیاده‌سازی مرجع صدور گواهی، خارج از حوزهٔ این پژوهش است و چون در هنگام این تحقیق، تلاش‌هایی برای راه‌سازی آن در کشور در شرف تصویب و آماده‌سازی بود، با فرض حضور مرجع عالی صدور گواهی دیجیتالی در جمهوری اسلامی ایران، مدل اعتماد این سیستم به صورت شکل (۳-٤) می‌باشد. برای انجام مبادلات الکترونیکی با خارج از کشور، توسط گواهی دیجیتالی که مرجع عالی صدور گواهی از مرجع صدور گواهی دیجیتالی بین‌المللی کسب نموده است، زنجیرهٔ اعتماد[1] بین موجودیتهای داخل و خارج کشور نیز فراهم می‌شود.

ساختار پایاچک و امضاها و گواهی‌های دیجیتالی الصاقی

۱ـ بخش ۱-۲ را ببینید.

شکل ۳-۴- سلسله مراتب مسؤولین گواهی در جمهوری اسلامی ایران

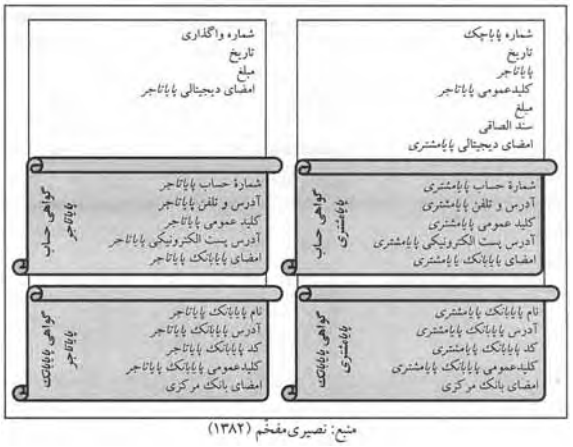


مرجع عالی صدور و تأیید گواهی دیجیتالی در جمهوری اسلامی ایران : IRCA
بانک مرکزی جمهوری اسلامی ایران – مرجع صدور گواهی دیجیتالی پایابانکها : CBCA
پایابانک – مرجع صدور گواهی دیجیتالی مشتریان پایابانک : PBCA
مشتریان پایابانک (پایامشتری، پایاتاجر) : C

منبع: نصیری‌مفخّم (۱۳۸۲)

با توجه به تعاریفی که در بخش ۳-۲-۳ بیان گردید، بر اساس مدل اعتماد مندرج در بخش ۳-۲-۵، نمای یک *پایاچک* مبادله شده بین *پایامشتری* و *پایاتاجر*، در شکل (۳-۵) آمده است.

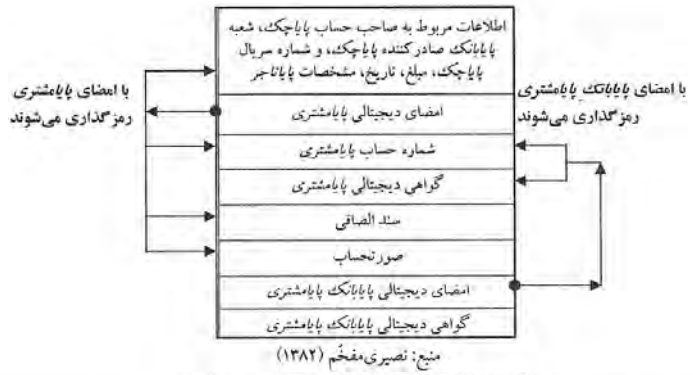
شکل ۳-۵- نمای یک *پایاچک* مبادله شده



منبع: نصیری‌مفخّم (۱۳۸۲)

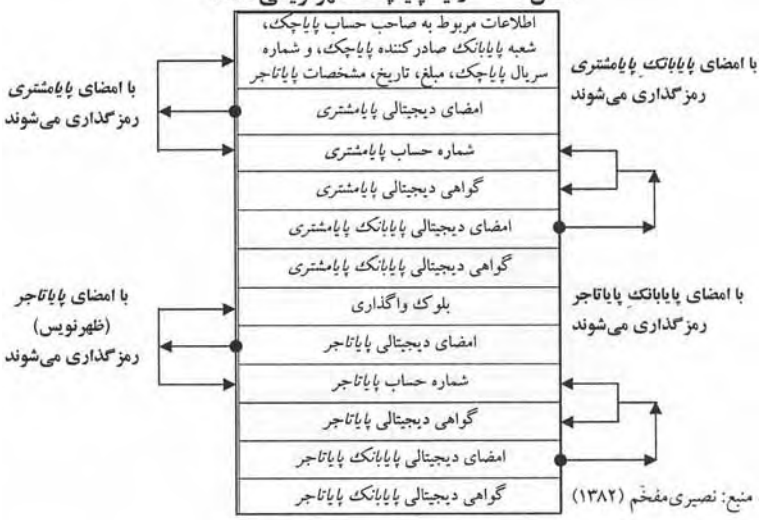
ساختار *پایاچک* و بخش‌هایی که توسط امضای *پایامشتری* و *پایابانک پایامشتری*، رمزگذاری می‌شود در شکل ۳-٦ نشان داده شده است. شکل (۳-۷) نیز، بخش‌های دیگری را که پس از امضا توسط *پایاتاجر* و *پایابانک پایاتاجر* درج می‌شود، نشان می‌دهد.

شکل۳-۶- ارایه *پایاچک*



منبع: نصیری‌مفخّم (۱۳۸۲)

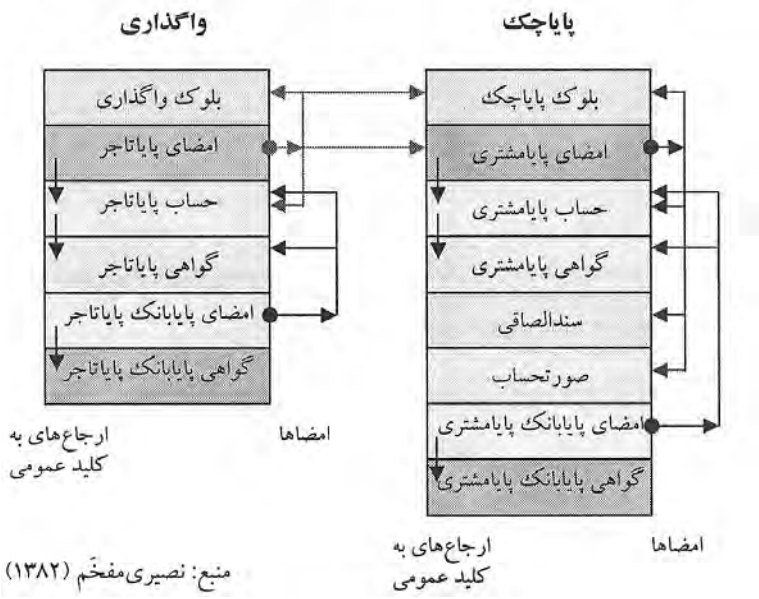
شکل۳-۷- ارایه *پایاچک* ظهرنویسی شده



منبع: نصیری‌مفخّم (۱۳۸۲)

در شکل ۳-۸ ارتباط بین امضاها و گواهی‌های روی *پایاچک* و واگذاری را مشاهده می‌کنیم.

شکل ۳-۸- ارتباط امضاها و گواهی‌های روی پایاچک و واگذاری



منبع: نصیری‌مفخَم (۱۳۸۲)

تعاریف و ساختار پروتکلهای سیستم پایاچک

در بخش ۳-۲-۳، تعاریف موجودیت‌های مطرح در سیستم *پایاچک* ارایه گردید. برای پایاچک، همانند چک فیزیکی چهار عملِ صدور دسته‌چک توسط بانک، نوشتن، امضا و ارسال پایاچک، واگذاریِ پایاچک توسط دریافت‌کننده، و نهایتاً پرداخت آن انجام می‌گیرد. برای این اعمال، پروتکل‌های «صدور کارت پایا و دسته‌چک پایا»، «صدور و امضای پایاچک برای خرید در پایابنگاه»، «واگذاری پایاچک در پایابانک» و «پرداخت پایاچک در پایابانک» طراحی شده است که در این بخش بیان می‌گردد[1].

۱ـ تفکر مورد استفاده در مکانیزم‌های امنیتی این پروتکل‌ها، از سناریویی که در بخش ۱-۲-۱ شرح آن آمد، شکل گرفته است.

در این پروتکل‌ها C، M، و B به ترتیب به عنوان پایامشتری، پایاتاجر و پایابانک به کار می‌روند. $Date_C$ تاریخی است که *پایامشتری*، *پایاچک* را می‌نویسد، و $Date_M$ تاریخی است که *پایاتاجر*، *پایاچک* را به *پایابانک* خود واگذار می‌کند. گواهی بانک مرکزی (برای خودش) را با $Cert_{BB}$، گواهی کلید عمومی کاربر C را با $Cert_C$، گواهی امضای *پایابانک* *پایامشتری* روی گواهی امضای *پایامشتری* را با $Cert_{B_C}[Cert_C]$، کلیدهای عمومی و خصوصی کاربری (زوج کلید کاربری) او در *پایابانک* را به ترتیب با pub_{1C} و prv_{1C}، کلیدهای عمومی و خصوصی امضای وی را به ترتیب با pub_{2C} و prv_{2C}، شناسهٔ او را با ID_C، شماره حساب را با ACC_C، شمارهٔ واگذاری *پایاچک* به پایاپانک را با SN۱، و شمارهٔ سریال صدور *پایاچک* را با SN۲ نشان می‌دهیم. PIN نیز به عنوان شمارهٔ محرمانهٔ دسترسی به کارت امضا و *دسته‌چک‌پایا* استفاده می‌شود. زوج کلید pub_{2C} و prv_{2C} و گواهی Cert۲ و شمارهٔ سریال SN۲ فقط برای دارندگان *دسته‌چک پایا* است و در کارت امضای دارندگانِ حساب‌های پس‌انداز قرار ندارد.

زوج کلید کاربری، فقط برای پیامهای بین *پایامشتری* و *پایابانک مشتری*، و زوج کلید امضا، برای پیامهای بین *پایامشتری* و سایرین استفاده می‌شود. پس کاربر C برای امضاکردن x، از $E_{prv_C}(x)$ و سایرین برای بررسی صحت این امضا از نماد $E_{pub_C}(E_{prv_C}(x))$ استفاده می‌کنند. رمزنمودن x برای کاربر C، توسط $E_{pub_C}(x)$ و رمزگشایی آن منحصراً توسط کاربر C به صورت $E_{prv_C}(E_{pub_C}(x))$ انجام می‌شود[۱].

در هر کدام از پروتکل‌های نوشتن و امضای چک از طرف پایامشتری، و واگذاری و ظهرنویسی از طرف پایاتاجر که از امضای دیجیتالی استفاده می‌شود، اطلاعات توسط کلید خصوصی درون کارت، امضا شده و گواهی‌های مربوطه نیز به آن ضمیمه می‌شود.

(الف) پروتکل صدور کارت امضا و دسته‌چک‌پایا

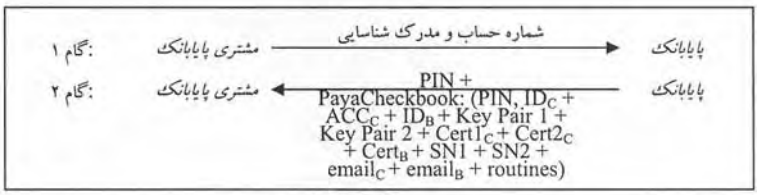
۲ـ گاهی اوقات در کتب و مقالات، وقتی کلید خصوصی برای امضا کردن x به کار می‌رود، از نماد Sign(x) و وقتی برای رمزگشایی x به کار می‌رود، از نماد D(x) استفاده می‌کنند. رمزنگاری و امضاهای دیجیتالی در بخش ۱-۲ آمده است.

چون بدون حضور فیزیکی، از ابتدا و مثلاً از طریق SSL و ارتباط ایمن از روی اینترنت، هویت‌شناسی ممکن نیست تا معلوم شود که ادعاکننده واقعاً همان صاحب حساب یا شخص دیگری است که اطلاعات حساب را دارد، لذا کاربری که برای نخستین بار، مایل به دریافت کارت پایا (*دسته‌چک‌پایا*) است، باید با مراجعه به یکی از شعب یک *پایابانک*، با تکمیل اطلاعات درخواستی و ارایه مدرک شناسایی معتبر، درخواست برخورداری از خدمات سیستم *پایاچک* را بنماید و در صورت نداشتن حساب، بایستی ابتدا اقدام به گشودن حساب (جاری) کند سرور *پایابانک*، یک آدرس پست الکترونیکی نهان[1]، در ارتباط با حسابی که سیستم هستهٔ بانکی برای متقاضی ایجاد کرده، تعریف می‌نماید و با صدور امضا و گواهی دیجیتالی به همراه شناسهٔ پایابانک و پایامشتری، شمارهٔ حساب، شمارهٔ سریال دسته‌چک‌پایا، و روتین‌های مربوطه، یک *دسته‌چک‌پایا*[2] روی یک وسیلهٔ دیجیتالی (کارت هوشمند، فلاپی) آماده کرده و به همراه دو شماره شناسایی محرمانه، به مشتری تحویل می‌دهد. یک شماره شناسایی مخصوص ورود به سیستم *پایاچک* از روی اینترنت است، و دیگر اینکه امکان استفاده از کارت برای امضا (/ و صدور *پایاچک*) را می‌دهد.

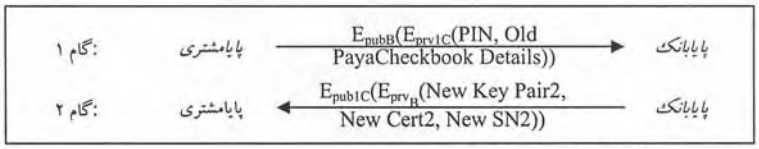
۱ـ همانگونه که در شکل ۳-۳ مشاهده کردیم، سرور پست الکترونیکی از بخش‌های مهم در ساختار یک پایابانک است. این سرور که حاوی اطلاعات پایاچک‌های صادره از/یا وارده به حساب دارندهٔ آن صندوق پستی الکترونیکی است، از طریق برنامه‌های کاربردی مربوطه، از طرف پایاکاربران مورد دسترسی قرار می‌گیرد. این سرور همچنین در ابتدای عضویت هر پایاکاربر در پایابانک، در ارتباط با سایر اجزای یک پایابانک، به همراه اطلاعات پایاکاربر، اقدام به ایجاد صندوق پست الکترونیکی و اعلام برای درج در گواهی الکترونیکی صادره می‌نماید (در واقع منظور از آدرس پست الکترونیکی نهان، آن است که فقط برنامه‌های کاربردی مربوطه در سمت *پایامشتری*، *پایابنگاه* و *پایابانک* از این آدرس استفاده می‌کنند). جزئیات این عملکرد در بخش‌های ٤-۱-۱-۱، ٤-۱-۱-۲ و ٤-۱-۱-۳ آمده است.

۲ـ بخش ۳-۲-۸ را نیز ببینید.

شکل ۳-۹- پروتکل (الف) درخواست و صدور غیرالکترونیکی کارت امضا و دسته‌چک *پایا* (ب) درخواست و صدور الکترونیکی کارت امضا و دسته‌چک *پایا*



(الف)



(ب)

منبع: نصیری‌مفخّم (۱۳۸۲)

پایامشتری (وقتی شمارهٔ سریال تعداد چکهای صادره از *دسته‌چک پایا* تمام شد)، می‌تواند از روی اینترنت توسط درخواست امضا شده‌ای، *دسته‌چک/کارت پایای* جدیدی را دریافت و بارگذاری نماید. پس این پروتکل برای هر پایاکاربر در اولین دفعهٔ استفاده، به صورت حضوری و برای دفعات بعدی به صورت اینترنتی است. ساختار این پروتکل برای درخواست غیرالکترونیکی/الکترونیکی صدور، در شکل ۳-۹ آمده است (در شکل ۳-۹-الف، مقادیر ID_C، ACC_C، و $email_C$ در واقع همراه $Cert1_C$ هستند و برای بیان حضور آنها، جداگانه نشان داده شده‌اند. مقادیر ID_B، و $email_B$ نیز همراه $Cert_B$ هستند).

(ب) پروتکل صدور *پایاچک* برای خرید در *پایابنگاه*

در مرحله نوشتن و امضای *پایاچک*، پروتکل شکل ۳-۱۰ انجام می‌شود. در این مرحله پس از اینکه *پایامشتری* روی پایابنگاه درخواست خرید داد، *پایاتاجر* صورتحساب را به *پایامشتری* می‌فرستد و *پایامشتری*، *پایاچک* را نوشته و امضا می‌نماید و او متقابلاً برای پایاتاجر می‌فرستد. بدیهی است با توجه به قانون چک، در هنگام صدور چک، باید وجه مربوطه در حساب موجود باشد، و صدور چک موعددار غیرقانونی است. بدین طریق امکان

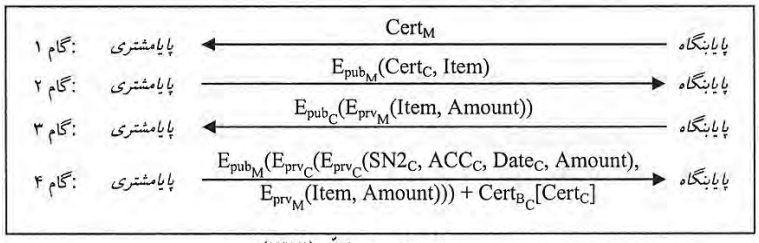
اجرای عملی این قانون، از طریق الکترونیکی شدن صدور چک میسر می‌گردد. این پروتکل شامل مراحل زیر است:

انتخاب کالا: گواهی *پایاتاجر* از روی پایابنگاه قابل دسترس است. *پایامشتری* برای پرداخت کالای مورد نظر در *پایابنگاه* با *پایاچک*، درخواست امضاشده‌ای (و در واقع گواهی امضای خود و آدرس) را با رمزنگاری کلید عمومی *پایاتاجر* به *پایابنگاه* (*پایاتاجر*) می‌فرستد (شکل ۳-۲، پیکان شمارهٔ صفر).

ارسال صورتحساب الکترونیکی: در ادامه *پایابنگاه*، به صورت خودکار، (مبلغ و) صورتحساب کالای مربوطه را امضا کرده و با کلید عمومی امضای *پایامشتری* (استخراج شده از گواهی دیجیتالی او) رمزنگاری نموده و به آدرس پستی نهان او ارسال می‌دارد. سرور *پایابانک پایامشتری*، به محض ارتباط *پایامشتری*، صورتحساب‌های وارده را نشان می‌دهد (شکل ۳-۲، پیکان شمارهٔ ۱).

صدور پایاچک: *پایامشتری*، پس از بررسی صحت پیام و امضای *پایاتاجر* (از روی گواهی او) روی صورتحساب وارده، اقدام به نوشتن یک *پایاچک* کرده و برای امضا و ارسال آن به همراه خلاصه‌ای از صورتحساب اولیه، از *دسته‌چک‌پایا* استفاده می‌کند و با رمزنگاری کلید عمومی پایاتاجر به آدرس پست الکترونیکی نهان او ارسال می‌نماید (شکل ۳-۲، پیکان شمارهٔ ۲).

شکل ۳-۱۰- پروتکل صدور *پایاچک*



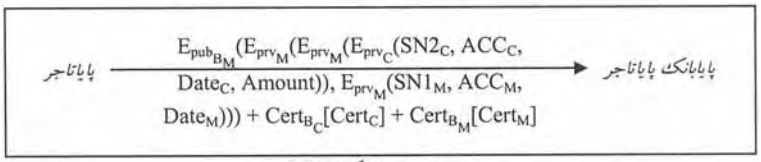
منبع: نصیری‌مفخّم (۱۳۸۲)

(ج) پروتکل واگذاری *پایاچک* در *پایابانک*

در *پایابنگاه*، به محض وصول *پایاچک*، پس از بررسی صحت پیام و امضای *پایامشتری* و صورتحساب الصاقی واصله، برای *پایا* چک جداشده از صورتحساب، فرمی جهت واگذاری به *پایابانک* تهیه شده و با امضای *پایاتاجر*

به *پایابانک* ارسال می‌شود (شکل ۳-۲، پیکان شمارهٔ ۳). سپس *پایابانکِ پایاتاجر*، دریافت آن را در فیلد وضعیت آن *پایاچک* برای *پایاتاجر* اعمال می‌کند که در حکم تأییدیهٔ دریافت *پایاچک* است (شکل ۳-۲، پیکان شمارهٔ ۱۱). شکل ۳-۱۱ این پروتکل را نشان می‌دهد.

شکل ۳-۱۱- پروتکل واگذاری *پایاچک*



منبع: نصیری‌مفخّم (۱۳۸۲)

(د) پروتکل پرداخت *پایاچک*: دریافت، پایاپای، و پرداخت *پایاچک* در *پایابانک*

در مرحله آخر، عمل پرداخت *پایاچک* انجام می‌گیرد. *پایابانکِ پایامشتری* پس از دریافت *پایاچک* ظهرنویسی شده، از شعبه‌هایی که *پایامشتری* در آنها حساب دارد، ماندهٔ حساب *پایامشتری* را جویا می‌شود، و تأیید یا عودت *پایاچک* را به اطلاع *پایابانکِ پایاتاجر* می‌رساند و مبلغ به حساب *پایاتاجر*، واریز و از حساب *پایامشتری* کسر می‌گردد. همچون روش سنتی، برای پرداخت پایاچک توسط (شعبهٔ) پایابانکِ پایامشتری، لازم است که اصل پایاچک به آن شعبه واصل گردد تا با دریافت پایاچک، مبلغ درخواستی را به (شعبهٔ) پایابانکِ پایاتاجر بپردازد. در صورتی که پایابانکِ پایامشتری، متمایز از پایابانکِ پایاتاجر باشد، لازم است که درخواست پایاپای، از طریق سویچ بین بانکی انجام شود. این پروتکل در شکل ۳-۱۲ آمده و شامل سه (و در حالت برگشتی بودن پایاچک، چهار) مرحلهٔ زیر است:

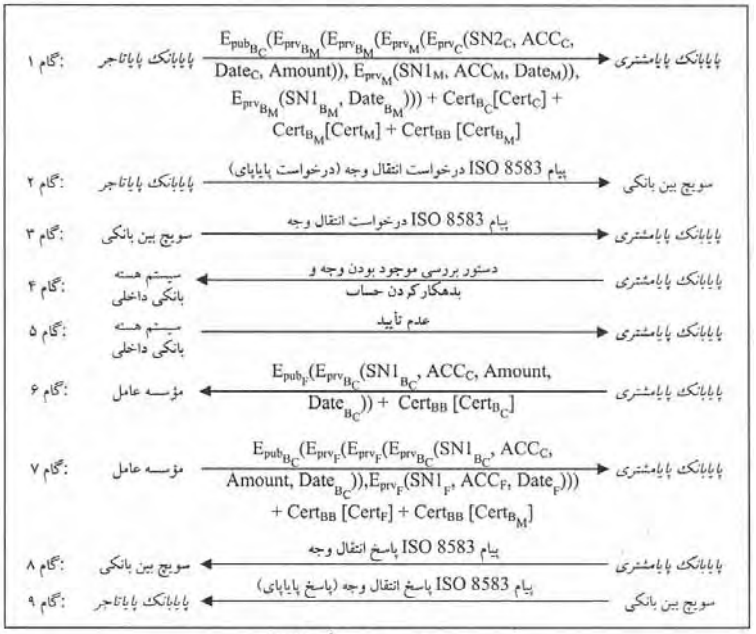
دریافت *پایاچک* در اولین *پایابانک* محل واگذاری (*پایابانکِ پایاتاجر*): به محض دریافت *پایاچک* در اولین *پایابانک* محل واگذاری، پس از بررسی صحت پیام و امضاهای روی آن (از طریق گواهی‌های الصاقی)، چنانچه

پایاچک مربوط به شعبه‌ای از همان *پایابانک* باشد، دستور مربوطه برای بدهکاری و بستانکاری *پایامشتری* و *پایاتاجر*، به قالب داده‌های سیستم هستهٔ بانکی ترجمه شده و به صورت ارتباط پیوسته بین دو شعبه اعمال شده و نتیجهٔ آن در فیلد وضعیت آن *پایاچک* برای هر دو طرف معامله اعمال و نشان داده می‌شود. این پروتکل در شکل ۳-۲ نشان داده نشده است.

پایاپای *پایاچک* با دومین *پایابانک* محل پرداخت (*پایابانکِ پایامشتری*): چنانچه *پایاچک* مربوط به *پایابانک* دیگری باشد، دستور مربوطه به قالب داده‌های سویچ بین بانکی ترجمه شده و از طریق سویچ، درخواست پایاپای می‌گردد (شکل ۳-۲، پیکان شمارهٔ ۵). در این صورت، اصل *پایاچک* با امضای اولین *پایابانک*، برای دومین *پایابانک* داده می‌شود (شکل ۳-۲، پیکان شمارهٔ ٤).

پرداخت *پایاچک* در *پایابانکِ پایامشتری*: *پایابانکِ پایامشتری با دریافت پیام پایاپای از سویچ بین بانکی و* دریافت *پایاچک* متناظر آن از طریق اینترنت از *پایابانک پایاتاجر*، پس از بررسی صحت *پایاچک* و امضاهای روی آن، پیام پایاپای را به دستورمربوطه برای بدهکاری *پایامشتری* به قالب داده‌های سیستم هستهٔ بانکی ترجمه کرده و به صورت ارتباط پیوسته، از شعبهٔ حساب *پایامشتری*، وضعیت حساب او را جویا می‌شود. چنانچه وجه کافی در حساب *پایامشتری* موجود باشد، حساب او را در آن شعبه بدهکار کرده و نتیجهٔ آن در فیلد وضعیت آن *پایاچک* در آدرس پست الکترونیکی نهان او اعمال و نشان داده می‌شود (شکل ۳-۲، پیکان شمارهٔ ۱۲) و دستور مربوطه از طریق سویچ بین‌بانکی برای اعمال در حساب *پایاتاجرِ پایابانک* اول نیز ارسال و اعمال می‌شود (پردازش درون *پایابانک*، در شکل ۳-۲ نشان داده نشده است).

شکل ۳-۱۲- پروتکل پرداخت *پایاچک* (این شکل، مربوط به سناریویی است که وجه کافی در حساب *پایامشتری* موجود نبوده ولی مؤسسهٔ عامل، پرداخت *پایاچک* او را پذیرد)



منبع: نصیری‌مفخّم (۱۳۸۲)

چکهای برگشتی و مؤسسهٔ عامل: چنانچه وجه کافی در حساب *پایامشتری* موجود نباشد، *پایابانک* با ارتباط با مؤسسهٔ عامل، وضعیت اعتبار *پایامشتری* را جویا می‌شود (شکل ۳-۲، پیکان شمارهٔ ۷). چنانچه اعتبار کافی داشته باشد، مؤسسهٔ عامل، وجه *پایاچک* را پرداخته و بقیهٔ آن مطابق پاراگراف قبل دنبال می‌شود. ولی در صورت عدم عضویت در مؤسسهٔ عامل یا عدم وجود اعتبار کافی در آن مؤسسه، نتیجهٔ آن در فیلد وضعیت آن *پایاچک* در آدرس پست الکترونیکی نهان *پایامشتری* اعمال و نشان داده می‌شود و دستور مربوطه از طریق سویچ بین بانکی برای اعمال در آدرس پست الکترونیکی نهان *پایاتاجرِ پایابانک* اول نیز ارسال و اعمال می‌شود (شکل ۳-۲، پیکان‌های شمارهٔ ۸، ۹، و ۱۰).

از شکل ۳-۱۲ استنباط می‌شود که پیام‌ها در گام‌های ۲، ۳، ۸ و ۹ که از ISO ۸۵۸۳ برای درخواست‌های انتقال وجه بین بانکی استفاده شده است، می‌توانسته دقیقاً مشابه گام‌های ٦ و ۷ مبادله شود. ولی استفاده از این روند

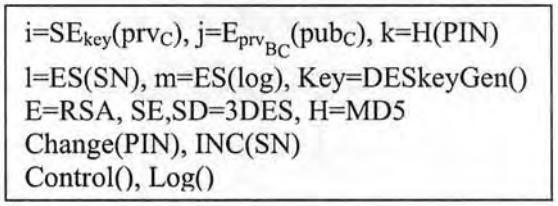
به دو دلیل صورت گرفته است: اول آنکه، شبکهٔ بانکی فقط دستورات واصله از شبکهٔ امن بانکی را به منظور پایاپای می‌پذیرد و این دستورات با قالب ISO ۸۵۸۳ و از طریق سویچ "شتاب" است. دوم آنکه، این روند باعث اطمینان بیشتراست. چراکه همچون جریان فیزیکی ارسال کارت‌های بانکی و ارسال PIN که از دو مسیر جداگانه صورت می‌گیرد تا به دست کاربر برسد و کسی که هر دو را داشته باشد قادر به استفاده از آن است، در اینجا نیز با قیاسی نه چندان دقیق، بررسی برای پرداخت وجه از طرف *پایابانک* *پایامشتری*، صرفاً موقعی صورت می‌گیرد که اصل دیجیتالی *پایاچک* را از طریق اینترنت و پیام درخواست پایاپای را از طریق سویچ بین بانکی دریافت کرده باشد.

شبیه‌سازی دسته‌چک‌پایا

همانگونه که در بخش ۳-۲-۲ و در تعریفی که در بخش ۳-۲-۳ برای *دسته‌چک‌پایا* آمد، برای کاربرد عملی سیستم *پایاچک*، استفاده از کارت‌های هوشمند،کارت‌های PCMCIA در کامپیوترهای کیفی و PDAها، سطح امنیت مناسبی را برای نگهداری اطلاعات مالی ایفا می‌کنند. در نمونه‌سازی این سیستم، عملکرد کارت هوشمند را روی فلاپی دیسک در نظر می‌گیریم.

شکل ۳-۱۳ شبیه‌سازی ساختار کارت هوشمند *دسته‌چک‌پایا* را روی فلاپی دیسک نشان می‌دهد. از آنجا که کلید عمومی کاربر در گواهی دیجیتالی صادره از *پایابانک* (j)، و کلید خصوصی او به صورت رمزشده (i) و صرفاً از طریق (کلید تولید شده از) PIN قابل دسترس است، لذا روتین‌هایی برای درهم‌سازی PIN (H) و رمزنگاری و رمزگشایی کلیدهای خصوصی و عمومی (SE_{key}, SD_{key}) لازم است. بدین صورت که PIN که به حالت درهم‌سازی‌شده (k) روی فلاپی است، با درهم‌سازی‌شدهٔ PIN وارده از طرف کاربر مقایسه می‌شود، و در صورت تطابق، امکان دسترسی به کلید خصوصی (prv_C) و احضار توابع مربوطه (E_{prv_C}) برای امضای سند مورد نظر فراهم می‌شود.

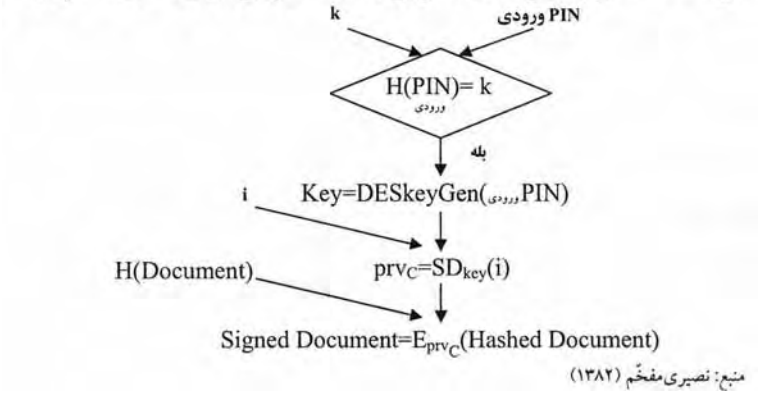
شکل ۳-۱۳- دسته‌چک پایا



منبع: نصیری‌مفخّم (۱۳۸۲)

رمز شدهٔ شماره سریال (l) و تابع افزایش آن (INC)، رمزشدهٔ تاریخچهٔ پایاچک‌های صادره (m) و تابع ثبت آن (Log)، تابع تغییر PIN (Change) و مکانیزم‌های کنترلی لازم (Control)، سایر اقلام موجود در دسته‌چک‌پایا هستند. تابع DESkeyGen نیز بر اساس پارامتر (PIN ورودی)، مقداری تولید می‌کند (که در صورت صحت PIN، دقیقاً همان است که در هنگام تولید کارت به عنوان کلید سری برای رمزنگاری متقارن اقلام کارت استفاده شده است) و می‌تواند به عنوان کلید برای رمزگشایی جهت دسترسی به کلید خصوصی به منظور امضا کردن استفاده شود. مکانیزم امنیتی امکان دسترسی به کلید خصوصی برای امضای سند پایاچک نیز در شکل ۳-۱٤ آمده است.

شکل ۳-۱۴- مکانیزم امنیتی امکان دسترسی به کلید خصوصی برای امضای سند *پایاچک*



منبع: نصیری‌مفخّم (۱۳۸۲)

برای امنیت از زیرساختار گواهی کلید عمومی با استاندارد X.۵۰۹ استفاده می‌شود. الگوریتم رمزنگاری کلید عمومی می‌تواند مثلاً RSA، و رمزنگاری متقارن، مثلاً ۳DES باشد. محدودیتی در الگوریتم مورد استفاده نیست و بسته به پیشرفت فناوری، می‌تواند با هر الگوریتم جدیدی جایگزین و صادر گردد.

فصل چهارم:
طراحی و پیاده‌سازی سیستم پایاچک

در سیستم‌های پیچیده، به دلیل آنکه نمی‌توانیم کل سیستم را یکجا درک کنیم، قبل از ساخت یا بازسازی چنین سیستم‌هایی، تجسم دیداری و مدل‌سازی، بسیار ضروری است. زبان مدل‌سازی یکپارچه[۱] (UML)، مستقل از زبان‌های برنامه‌نویسی خاص و فرایندهای توسعه، بر یک زبان مدل‌سازی استاندارد استوار است و از یک فرامدل[۲] و نمادهای علامت‌گذاری استفاده می‌کند. از آنجا که سیستم‌های تجارت الکترونیکی در محیط‌های شیءگرا و مبتنی بر اجزاء تهیه می‌شوند و باید با کاربردهای موجود در شرکت‌های متفاوت و روی محیط‌های متفاوت و با زبان‌های متفاوت سازگار باشند، UML، راهکار طراحی مدل چنین سیستم‌هایی است. دیدگاه‌هایی که UML برای تحلیل و توسعه سیستم فراهم می‌آورد، عبارت از نمودار مورد کاربرد[۳]، نمودار کلاس[٤]، نمودارهای رفتار[٥] (نمودار حالت[٦]، نمودار فعالیت[۷])، نمودارهای تعامل[۸] (نمودار توالی[۹]، نمودار همکاری[۱۰])، و نمودارهای پیاده‌سازی[۱۱] (نمودار اجزا[۱۲]، نمودار استقرار[۱۳]) هستند. ارتباطات در دیدگاه شیءگرا به سه دستهٔ کلی تعمیم، تناظر، و

---

۱. **Unified Modeling Language**
۲. **metamodel**
۳. **Use Case Diagram**
٤. **Class Diagram**
٥. **Behavior Diagrams**
٦. **State Chart Diagram**
۷. **Activity Diagram**
۸. **Interaction Diagram**
۹. **Sequence Diagram**
۱۰. **Collaboration Diagram**
۱۱. **Implementation Diagram**
۱۲. **Component Diagram**
۱۳. **Deployment Diagram**

وابستگی، تقسیم می‌شوند. این ارتباطات بین موارد کاربرد، کنش‌گر[۱]، کلاس‌ها یا واسط‌ها استفاده می‌شوند (احمد، ۲۰۰۲؛ فاولر، ۲۰۰۰؛ ساعدی، ۱۳۷۹).

از دیدگاه فرایند مدلسازی عقلائی[۲] (RUP)، برای توسعهٔ یک سیستم عملی، شش مرحلهٔ اصلی مدلسازی تجاری، تحلیل خواسته‌ها، تحلیل و طراحی، پیاده‌سازی، آزمون، و استقرار باید طی شود (احمد، ۲۰۰۲). در این تحقیق، تا اینجا با بررسی و ارزیابی سیستم‌های پرداخت الکترونیکی با توجه به جنبه‌های بانکی، اقتصادی، حقوقی و اجتماعی مربوطه و بیان مشکلات و نیازها و اولویت‌های مطرح در کشور، با ارایهٔ سیستم *پایاچک*، مراحل مدل‌سازی تجاری، تحلیل خواسته‌ها و تحلیل این سیستم را پشت سر گذاشتیم و در این فصل، مدل سیستم *پایاچک* را که در فصل سوم ارایه نمودیم، با زبان UML توسط Rational Rose Enterprise Edition ۲۰۰۲ طراحی می‌نماییم.

طراحی مدل پیشنهادی سیستم پایاچک

در فصل سوم، مدل سیستم پیشنهادی *پایاچک* را برای پرداخت اینترنتی در ایـران با استفاده از چک الکترونیکی تشریح گردید. براساس تعاریفی که از موجودیت‌ها و فرایندهای این سیستم بیان شد تعریف سیستم *پایاچک* به اختـصار و بـدون ورود بـه جـزئیات، آن اسـت که یک *پایامشتری* از روی *پایابـنگاه* یـک *پایاتاجـر*، توسـط *دسته‌چک‌پایای* دریافتی از یک *پایابانک*، با *پایاچک* خرید می‌کند.

جـزئیات قـضیه، در *دسـته‌چـک‌پایـا*/کارت امضای پایا و *پایابانک* نهفته اسـت. *دسـته‌چـک‌پایـا*/کـارت امضای پایا به عنوان مجوز صدور/واگذاری *پایاچـک* است و *پایابانک*‌ها، با مجوز بانک مرکزی، اعطاکنندهٔ این مجوز از طـریق صـدور امـضاها و گواهی‌های دیجیتالی هستند. درسمت *پایابانک*‌ها،

---

۱. Actor
۲. Rational Unified Modeling Process

سـویچ بـین بانکی، حساب‌های دوبانک نزد بانک پایاپای (بانک مرکزی) را پایاپـای مـی‌کـند. مؤسـسهٔ عامـل نیـز برای حفظ شناوری *پایاچک*‌ها برای متقاضـیان ایـن خـدمات، در کـنار *پایابانک پایامشتری* انجام وظیفه می‌کند. نمـای کلـی مـدل ایـن سیـستم، در شـکل ۳-۲ و پروتکل‌های مربوطه، در شکل‌های ۳-۹ تا ۳-۱۲ آمده است.

در ادامـه، طراحـی نمـودارهای مـدل سیـستم *پایـاچک* با نیم نگاهی به بخـش ۳-۲ ارایـه مـی‌گـردد. در هـر پروژه‌ای برای تسلط بر نیازمندی‌ها و بـرنامه‌ریـزی و کنتـرل پروژه، ابتدا باید کاربران و موارد کاربرد را شناسایی کرد و سپس شروع به مدل‌سازی نمود.

نمودارهای مورد کاربرد سیستم پایاچک

می‌دانیم که نمودارهای مورد کاربرد، برای نمایش نیازها و انتظارات کاربر از سیستم هستند. کاربران سیستم، کنش‌گرهایی هستند که با سیستم برهم‌کنش دارند. برای شناسایی کنش‌گرهای سیستم، ابتدا باید به این سؤالها پاسخ دهیم: چه کسی از این عملکرد استفاده می‌کند؟ چه کسی اطلاعات بدست می‌آورد؟ چه کسی می‌تواند اطلاعات را تغییر دهد؟ آیا سیستم‌های دیگری با این سیستم برهم‌کنش دارند؟

در سیستم *پایاچک*، نقش‌هایی که پاسخ این سؤالات هستند، *پایامشتری*، *پایاتاجر* (و *پایابنگاه*)، *پایابانک* (دروازهٔ *پایاچک*، سیستم هستهٔ بانکی، سیستم پست الکترونیکی، سیستم مرجع گواهی، سیستم واسط سویچ بین بانکی)، بانک پایاپای، سویچ بین بانکی، مؤسسهٔ عامل، و *دسته‌چک‌پایا* (*کارت‌امضای‌پایا*) هستند. تعاریف این نقش‌ها در بخش ۳-۲-۳ آمده است و فقط یادآوری می‌شود که یک *پایامشتری* با داشتن یک حساب جاری در یک *پایابانک*، دارای *دسته‌چک‌پایا* جهت صدور و امضای *پایاچک*، و یک *پایاتاجر*، با داشتن هرگونه حسابی در یک پایابانک، دارای یک *کارت‌امضای‌پایا* برای دریافت و واگذاری *پایاچک* در *پایابانک* است.

موارد کاربرد سیستم، برگرفته از پروتکل‌هایی است که در بخش ۳-۲-۲ به اختصار و در بخش ۳-۲-۷ به تفصیل تعریف گردیدند. اهم این موارد کاربرد، در شکل ٤-۱ آمده است و به تفکیک در بخش‌های زیر بیان می‌گردند.

مورد کاربرد: درخواست صدور *کارت‌امضای‌پایا*

همانگونه که در فصل سوم گفته شد، از آنجا که بدون حضور فیزیکی، از ابتدا و مثلاً از طریق SSL و ارتباط ایمن از روی اینترنت، هویت‌شناسی برقرار نیست که معلوم شود که ادعاکننده واقعاً همان صاحب حساب یا شخصی دیگر است که اطلاعات حساب را دارد، لذا صدور *کارت‌امضای‌پایا*، برای اولین بار به صورت حضوری و تمدید آن، به صورت اینترنتی انجام می‌شود. این مورد کاربرد، برگرفته از پروتکل ۳-۲-۷-الف است.

مورد کاربرد (الف): صدور *کارت‌امضای‌پایا* به صورت حضوری

برای مورد کاربرد صدور *کارت‌امضای‌پایا* به صورت حضوری، مراحل زیر باید طی شود:

۱) *پایاتاجر* با مراجعه حضوری به یک *پایابانک*، درخواست صدور *کارت‌امضای پایا* می‌کند.

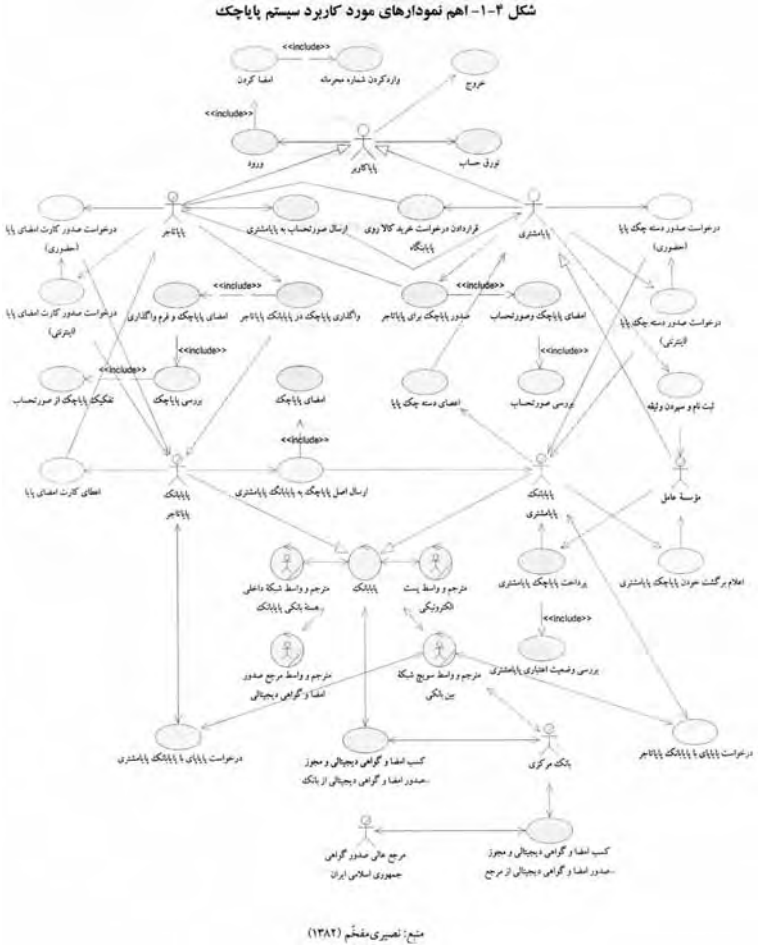
۲) *پایابانک* از او می‌خواهد که برای افتتاح یک حساب، فرم اطلاعات لازم را تکمیل کند.

۳) *پایاتاجر* با ارایه مدرک شناسایی معتبر، اطلاعات لازم را مشخص می‌کند.

٤) *پایابانک*، با ایجاد یک شماره حساب و آدرس پست الکترونیکی، و کلیدها و گواهی‌های امضا، همراه با مشخصات پایاتاجر و پایابانک، یک *کارت‌امضای‌پایا* حاوی اقلام فوق‌الذکر را روی وسیلهٔ الکترونیکی (کارت هوشمند، فلاپی دیسک، ...) ایجاد می‌کند.

۵) پایابانک، یک شمارهٔ شناسایی محرمانه برای دسترسی به کارت امضا، در درون کارت قرار داده و به صورت محرمانه به همراه کارت‌امضای‌پایا، به پایاتاجر تحویل می نماید.

شکل ۴-۱- اهم نمودارهای مورد کاربرد سیستم پایاچک



منبع: نصیری‌مقدّم (۱۳۸۲)

مورد کاربرد (ب): صدور *کارت‌امضای‌پایا* به صورت اینترنتی

برای مورد کاربرد صدور *کارت‌امضای‌پایا* به صورت اینترنتی، مراحل زیر باید طی شود:

۱) *پایاتاجر* با مراجعه اینترنتی به پایابانک خود، درخواست تمدید *کارت‌امضای‌پایا* برای حساب خود را می‌کند.

۲) *پایابانک* از او می‌خواهد که درخواست خود را با «کلید امضای کاربری[1]» امضا کند.

۳) *پایاتاجر*، درخواست تمدید گواهی امضای حساب را با کلید امضای کاربری خود امضا کرده و به *پایابانک* ارسال می‌کند.

٤) در صورتی‌که منقضی شدن گواهی، صرفاً مربوط به سرآمدن مدت اعتبار آن باشد، *پایابانک*، گواهی تمدید شدهٔ امضای حساب *پایاتاجر* را امضا کرده و برای *پایاتاجر* ارسال می‌کند.

۵) *پایاتاجر*، گواهی تمدید شدهٔ امضای حساب را دریافت و روی وسیلهٔ الکترونیکی خود بارگذاری می‌نماید.

مورد کاربرد دیگر، مربوط به هنگامی است که گواهی امضای حساب به دلایلی همچون اعلام موضوع مفقودشدن یا جعل آن به *پایابانک*، پیش از موعد، منقضی گردیده باشد، که در این صورت، تمدید انجام نشده و به اطلاع *پایاتاجر* رسانده می‌شود. ادامهٔ استفاده از این حساب منوط به مراجعهٔ حضوری مدعی به *پایابانک* است که مشخص شود که دارندهٔ کارت امضا، همان شخصی است که ادعا می‌کند (و شماره محرمانه و خود کارت را به صورت غیر قانونی تصاحب نکرده است). در صورت صحت، پایابانک گواهی را تمدید کرده و روی کارت، بارگذاری و به پایاتاجر تحویل می‌نماید.

مورد کاربرد: درخواست صدور *دسته‌چک‌پایا*

به همان دلایلی که در بخش ٤-۱-۱-۱ اشاره گردید، صدور *دسته‌چک‌پایا*، برای اولین بار به صورت حضوری و تمدید آن، به صورت اینترنتی است. این مورد کاربرد، برگرفته از پروتکل ۳-۲-۷-الف است.

مورد کاربرد (الف): صدور *دسته‌چک‌پایا* به صورت حضوری

برای مورد کاربرد صدور *دسته‌چک‌پایا* به صورت حضوری، مراحل زیر باید طی شود:

۱) *پایامشتری* با مراجعه حضوری به یک *پایابانک*، درخواست صدور *دسته‌چک‌پایا* می‌کند.

۲) *پایابانک* از او می‌خواهد که برای افتتاح یک حساب جاری، فرم اطلاعات لازم را تکمیل کند.

۱ـ بخش ۳-۲-۲ و ۳-۲-۷ را ببینید.

۳) *پایامشتری* با ارایه مدرک شناسایی معتبر، اطلاعات لازم را مشخص می‌کند.

٤) *پایابانک*، طی ارتباط پیوسته و استعلام از بانک مرکزی، در صورت دریافت پاسخ مبنی بر صحت شرایط *پایامشتری*، با ایجاد یک شماره حساب جاری و آدرس پست الکترونیکی، و کلیدها و گواهی‌های امضا، همراه با مشخصات *پایامشتری* و *پایابانک*، یک *دسته‌چک‌پایا* حاوی اقلام فوق‌الذکر را روی وسیلهٔ الکترونیکی (کارت هوشمند، فلاپی دیسک، ...) ایجاد می‌کند.

۵) *پایابانک*، یک شمارهٔ شناسایی محرمانه برای دسترسی به *دسته‌چک پایا*، به صورت محرمانه به همراه *دسته‌چک‌پایا*، به *پایامشتری* تحویل می‌نماید.

مورد کاربرد (ب): صدور *دسته‌چک‌پایا* به صورت اینترنتی

برای مورد کاربرد صدور *دسته‌چک‌پایا* به صورت اینترنتی، مراحل زیر باید طی شود:

۱) *پایامشتری* با مراجعه اینترنتی به *پایابانک* خود، درخواست تمدید *دسته‌چک‌پایا* برای حساب جاری خود را می‌کند.

۲) *پایابانک* از او می‌خواهد درخواست خود را با «کلیدامضای‌کاربری» امضا کند.

۳) *پایامشتری* درخواست تمدید گواهی امضای حساب جاری را با کلیدامضای‌کاربری خود امضا کرده و به *پایابانک* ارسال می‌کند.

٤) در صورتی‌که منقضی شدن گواهی، صرفاً مربوط به سرآمدن مدت اعتبار آن باشد، *پایابانک*، گواهی تمدید شدهٔ امضای حساب *پایامشتری* را امضا کرده و برای *پایامشتری* ارسال می‌کند.

۵) *پایامشتری*، گواهی تمدید شدهٔ امضای حساب جاری را دریافت و روی وسیلهٔ الکترونیکی خود بارگذاری می‌نماید.

مورد کاربرد دیگر، مربوط به هنگامی است که گواهی امضای حساب به دلایلی همچون اعلام مفقود شدن یا جعل آن، یا معلوم شدن سابقهٔ بدحسابی و چک‌های برگشتی با استعلام از بانک مرکزی، پیش از موعد منقضی گردیده باشد، که در این صورت، تمدید انجام نشده و موضوع به اطلاع *پایامشتری* رسانده می‌شود. ادامهٔ استفاده از این حساب منوط به مراجعهٔ حضوری مدعی به *پایابانک* است که مشخص شود که دارندهٔ *دسته‌چک‌پایا* همان شخصی است

که ادعا می‌کند (و شماره محرمانه و خود کارت را به صورت غیر قانونی تصاحب نکرده است). در صورت صحت، گواهی توسط پایا بانک تمدید شده و روی کارت بارگذاری و به *پایامشتری* تحویل می‌گردد.

مورد کاربرد: صدور *کارت‌امضای‌پایا/دسته‌چک‌پایا* در *پایابانک*

همانگونه که شکل ۳-۳ نمای یک *پایابانک* را نشان می‌دهد، در محل هر *پایابانک* سیستم‌هایی باهم در ارتباط هستند. در واقع برای گام چهارم در موارد کاربرد ٤-۱-۱-۱-الف و ٤-۱-۱-۲-الف مراحل زیر، باید طی گردد:

۱) دروازهٔ *پایاچک*، اطلاعات *پایاکاربر* (*پایامشتری*/*پایاتاجر*) را برای افتتاح حساب، به هستهٔ بانکی *پایابانک* می‌دهد.

۲) سیستم هستهٔ بانکی *پایابانک*، یک شماره حساب ایجاد می‌کند و به دروازهٔ *پایاچک* می‌دهد.

۳) دروازهٔ *پایاچک*، اطلاعات و شماره حساب را به سیستم پست الکترونیکی *پایابانک* می‌دهد.

٤) سیستم پست الکترونیکی *پایابانک*، یک آدرس پست الکترونیکی در ارتباط با این اطلاعات و شماره حساب ایجاد می‌کند و به دروازهٔ *پایابانک* می‌دهد.

۵) دروازهٔ *پایابانک*، اطلاعات، شماره حساب و آدرس پست الکترونیکی *پایاکاربر* را به سیستم مرجع گواهی می‌دهد.

٦) سیستم مرجع گواهی *پایابانک*، کلیدهای امضا را صادر نموده و بر اساس مشخصات *پایاکاربر*، اطلاعات حساب و *پایابانک*، و آدرس پست الکترونیکی، گواهی مربوط را صادر می‌کند. این اطلاعات با یک شمارهٔ شناسایی، محرمانه شده و روی وسیلهٔ الکترونیکی قرار داده می‌شود. شمارهٔ شناسایی به همراه *دسته‌چک‌پایا*/*کارت‌امضای‌پایا* به *پایاکاربر* تحویل داده می‌شود.

مورد کاربرد: صدور و امضای پایاچک برای خرید در پایابنگاه

برای آنکه پایامشتری مطمئن باشد که *پایاچک* را برای پرداختن قیمت مندرج در صورتحسابی می‌نویسد که درست و دقیقاً متعلق به خود اوست، لازم است که پایامشتری و پایاتاجر پیامهای مبادله شده را امضا کرده و با کلید عمومی طرف مقابل، رمزنگاری کنند. بررسی صحت امضاها از طریق گواهی کلید امضا که به طرف مقابل می‌دهند، قابل بررسی است. کلید عمومی و

گواهی پایاتاجر از روی پایابنگاه برای پایامشتری قابل حصول است. اما برای آنکه پایاتاجر بتواند صورتحسابی محرمانه فقط به شخص پایامشتری بدهد، پایامشتری باید با بازدید از پایابنگاه و انتخاب کالا، روی درخواست خود را امضا و گواهی نماید. پس با این توضیحات، این مورد کاربرد که برگرفته از پروتکل ۳-۲-۷-ب است، حاوی مراحل زیر می‌باشد:

۱) پایامشتری پس از تورق پایابنگاه و انتخاب کالا، با دسترسی به کلیدعمومی و گواهی پایاتاجر، درخواست امضاشده‌ای برای این کالا به پایابنگاه می‌فرستد.

۲) پایابنگاه، پس از دسترسی به کلید عمومی و گواهی امضای پایامشتری از روی درخواست او، پس از اطمینان نسبت به صحت امضا و جامعیت آن درخواست، صورتحساب این کالا را امضا و برای پایامشتری، رمزنگاری نموده و به آدرس او ارسال می‌کند.

۳) پایامشتری پس از اطمینان از صحت امضا و جامعیت صورتحساب، اقدام به نوشتن پایاچک برای مبلغ مندرج در صورتحساب کرده، آن را امضا نموده و پس از الصاق صورتحساب، کل آن را مجدداً امضا و برای پایابنگاه، رمزنگاری و ارسال می‌کند.

٤) پایاتاجر، دریافت پایاچکِ امضا شده و صورتحساب را به پایامشتری اعلام می‌کند.

اگر در هرکدام از مراحل، فوق‌الذکر صحت امضا یا جامعیت پیام تأیید نشود، در آن صورت مورد کاربرد با اعلام به شخص ذی‌نفع، پایان می‌یابد.

شایان ذکر است که در همهٔ موارد کاربردی که نیاز به امضای دیجیتالی پایاکاربر/پایابانک است، مورد کاربردی مشترک وجود دارد که برای قراردادن و ورود شمارهٔ محرمانهٔ وسیلهٔ الکترونیکیِ امضا، درخواست می‌نماید، و *پایاکاربر/پایابانک*، شمارهٔ محرمانه را برای دسترسی به امضا وارد می‌کند.

مورد کاربرد: واگذاری پایاچک در پایابانک

این مورد کاربرد، برگرفته از پروتکل ۳-۲-۷-ج و شامل مراحل زیر است:

۱) پایاتاجر پس از اطمینان از صحت امضا و جامعیت پایاچک و صورتحساب، پایاچک را استخراج کرده و اقدام به نوشتن فرم واگذاری و

امـضای آن نموده و پس از الصاق این فرم به پایاچک، کل آن را مجدداً امضا و برای پایابانک، رمزنگاری و ارسال می‌کند.

۲) پایابانک، دریافت پایاچک واگذار شده را به پایاتاجر اعلام می‌کند.

مورد کاربرد: پرداخت پایاچک در پایابانک

همانگونه که در شکل ۳-۲ مشاهده می‌شود، همچون روش سنتی، برای پرداخت پایاچک توسط (شعبهٔ) پایابانک پایامشتری، لازم است که اصل پایاچک به آن شعبه واصل گردد تا با دریافت پایاچک، مبلغ درخواستی را به (شعبهٔ) پایابانک پایاتاجر بپردازد. در صورتی که پایابانک پایامشتری، متمایز از پایابانک پایاتاجر باشد، باید درخواست پایاپای، از طریق سویچ بین بانکی انجام شود. این مورد کاربرد، برگرفته از پروتکل ۳-۲-۷-د است.

مورد کاربرد (الف): پرداخت پایاچک در شعب یک پایابانک

این مورد کاربرد، طبق مراحل زیر صورت می‌گیرد:

۱) پایابانک پایاتاجر پس از اطمینان از صحت امضاها و جامعیت پایاچک و فرم واگذاری، پایاچک را استخراج می‌کند.

۲) پایابانک پایاتاجر، اصل پایاچک را برای پایاپای، به شعبهٔ پایابانک پایامشتری ارسال می نماید.

۳) چنانچه پایاچک، متعلق به همان شعبهٔ پایابانک (یا شعبه‌ای دیگر از همان پایابانک) باشد، پایابانک پایا تاجر، دستور بدهکاری و بستانکاری حساب‌های پایامشتری و پایاتاجر را به صورت دستورات درون سیستم هستهٔ بانکی آن پایابانک ترجمه می‌کند.

٤) این دستور به صورت ارتباط پیوسته روی حساب‌ها در دو شعبهٔ مربوطه اعمال و پایاپای می‌شود.

۵) نتیجه به پایاتاجر و پایامشتری اعلام می‌شود.

مورد کاربرد (ب): پرداخت پایاچک در (شعب) دو پایابانک متمایز

این مورد کاربرد، طبق مراحل زیر صورت می‌گیرد:

۱) پایابانک پایاتاجر پس از اطمینان از صحت امضاها و جامعیت پایاچک و فرم واگذاری، پایاچک را استخراج می‌کند.

۲) اصل پایاچک را برای پایاپای، به شعبهٔ پایابانک پایامشتری ارسال می‌نماید.

۳) چنانچه پایاچک، متعلق به شعبه‌ای از پایابانک دیگر باشد، پایابانک تاجر، دستور بدهکاری و بستانکاری حساب‌های پایامَشتری و پایاتاجر را بهَ صورت (پیام‌های) دستورات سویچ بین بانکی ترجمه و از طریق سویچ، درخواست پایاپای می‌کند.

٤) پایابانک پایامشتری با دریافت توأم اصل پایاچک از طریق اینترنت و پیام درخواست پَایاپای از طریق سویچ بین بانکی، صحت امضاها و جامعیت پایاچک را بررسی می‌کند، و در صورت تأیید، دستور بدهکاری حساب پایامشتری را به صورت دستورات درون سیستم هستهٔ بانکی پایابانک ترجمه می‌کند.

۵) توسط این دستور، موجود بودن وجه در حساب پایامشتری، با داشتن ارتباط مستمر و پیوسته با شعبهٔ مربوطه بررسی می‌شود.

٦) در صورت وجود وجه کافی در حساب پایامشتری، حساب او بدهکار می‌شود.

۷) پایابانک پایامشتری، نتیجه را به پایامشتری اعلام می‌کند.

۸) پیام اعلاَم بدهکار شدن حساب پایامشتری، به قالب سویچ بین بانکی ترجمه و از طریق سویچ، به پایابانک پایاتاجر ارسال می‌شود.

۹) پایابانک پایاتاجر، بر اسَاس پیام دریافتی از سویچ مبنی بر بدهکار شدن حساب پایاَمشتری، دستور بستانکاری حساب پایاتاجر را به صورت دستورات درون سیستم هستهٔ بانکی پایابانک ترجمه می‌کند.

۱۰) این دستور به صورت ارتباط پیوسته روی حساب پایاتاجر در شعبهٔ مربوطه اعمال و پایاپای می‌شود.

۱۱) پایابانک پایاتاجر، نتیجه را به پایاتاجر اعلام می‌کند.

مشاهده می‌شَود که این مورد کاربرد در واقع ترکیبی از سه مورد کاربرد مجزا است. مراحل ۱ تا ۳، ٤ تا ۸، و ۹ تا ۱۱ می‌توانند به سه مورد کاربرد تفکیک شوند.

مورد کاربرد (ج): پرداخت پایاچک در پایابانک با واسطهٔ مؤسسهٔ عامل

در واقع این مورد کاربرد، حالت خاصی از هر دو مورد کاربرد پیشین است. در مرحله چهارم از مورد کاربرد ٤-۱-۱-٦-الف و مرحله ششم از مورد

کاربرد ٤-١-١-٦-ب، چنانچه وجه کافی در حساب پایامشتری موجود نباشد، این مراحل دنبال می‌شود:

۱) پایابانک پایامشتری، با پیامی امضا شده و رمزنگاری شده برای مؤسسهٔ عامل، موضوع برگشت‌خوردن پایاچک روی حساب پایامشتری را به او اعلام می‌کند.

۲) مؤسسهٔ عامل، پس از اطمینان از صحت امضا و جامعیت پیام پایابانک پایامشتری، پیام را به صورت دستورات درون سیستم اطلاعاتی خود ترجمه می‌کند.

۳) چنانچه پایامشتری، در این مؤسسه ثبت‌نام کرده باشد و وضعیت او از نظر این مؤسسه برای مبلغ پایاچک مورد تأیید باشد، (مطابق محاسبات مندرج در آیین‌نامهٔ مربوط، که پایامشتری در موقع ثبت‌نام، از شرایط آن آگاه شده است) از اعتبار پایامشتری کسر شده و در سیستم اطلاعاتی ثبت می‌شود.

٤) دستور پرداخت جهت بدهکاری حساب مؤسسهٔ عامل و بستانکاری حساب پایامشتری، با پیامی امضا و رمزنگاری شده برای پایابانک پایامشتری ارسال می‌شود.

۵) پایابانک پایامشتری، پس از اطمینان از صحت امضا و جامعیت پیام مؤسسهٔ عامل، پیام را به صورت دستورات درون سیستم هستهٔ بانکی پایابانک ترجمه می‌کند.

٦) توسط این دستور به صورت ارتباط پیوسته با شعبهٔ مربوطه، حساب مؤسسهٔ عامل، بدهکار و حساب پایامشتری، بستانکار می‌شود.

۷) در دستور دیگری، حساب پایامشتری بابت پایاپای با حساب پایاتاجر، بدهکار می‌شود.

۸) پایابانک پایامشتری، نتیجه را به پایامشتری اعلام می‌کند.

۹) پیام اعلام بدهکار شدن حساب پایامشتری، به قالب سویچ بین بانکی ترجمه و از طریق سویچ، به پایابانک پایاتاجر ارسال می‌شود.

۱۰) پایابانک پایاتاجر، بر اساس پیام دریافتی ازسویچ، مبنی بر بدهکار شدن حساب پایامشتری، دستور بستانکاری حساب پایاتاجر را به قالب دستورات درون سیستم هستهٔ بانکی پایابانک ترجمه می‌کند.

۱۱) ایـن دسـتور به صورت ارتباط پیوسته روی حساب پایاتاجر در شعبهٔ مربوطه اعمال و پایاپای می‌شود.

۱۲) پایابانک پایاتاجر، نتیجه را به پایاتاجر اعلام می‌کند.

مورد کاربرد دیگر، مربوط به هنگامی است که مؤسسهٔ عامل، پرداخت وجه پایاچک پایامشتری را متقبل نشود، که در این صورت، پیام پرداخت نشدن پایاچک، با امضا و رمزنگاری به پایامشتری اعلام، و نیز با ترجمه به قالب سویچ بین بانکی، و از طریق سویچ به پایابانک پایاتاجر ارسال می‌شود. خود پایاچک نیز به صورت امضا و رمزنگاری شده برای پایابانک پایاتاجر، به او برگشت داده می‌شود. پایابانک پایاتاجر با دریافت توأم پایاچک از طریق اینترنت، و پیام برگشت پایاچک ازطریق سویچ بین بانکی، صحت امضاها و جامعیت پایاچک را بررسی می‌کند. در صورت صحت، نتیجه به پایاتاجر اعلام می‌شود و اصل پایاچک با امضا و رمزنگاری به پایامشتری برگشت داده می‌شود.

مورد کاربرد: ورود به سیستم *پایاچک*

هر چند این مورد کاربرد، به خودی خود یک مورد کاربرد نیست، اما در مورد کاربردهایی که در فوق ذکر شد، استفاده می شود.

به پایاکاربر اعلام می‌شود که نام و رمز عبور خود را وارد نماید (رمز عبور، با کلید امضای کاربری پایاکاربر، امضا شده و با کلید عمومی پایابانک، رمزنگاری و ارسال می‌شود). سیستم پایاچک، با بررسی امضا و جامعیت پیام، تحقیق می‌کند که این پایاکاربر وجود دارد و رمز عبور وارد شده برای این پایاکاربر، معتبر است. سیستم، صفحهٔ اصلی سیستم پایاچک را نشان می‌دهد که پایاکاربر بتواند فعالیت‌های خود را در پایابانک انجام دهد.

مورد کاربرد دیگر، مربوط به هنگامی است که پایاکاربر، پایاکاربر سیستم پایاچک این پایابانک نباشد و یا امضا یا جامعیت و صحت رمز عبور، نامعتبر باشد؛ در این صورت، یک پیغام خطا به پایاکاربر نشان داده می‌شود و به او مجدداً فرصت داده می‌شود که برای وارد شدن، تلاش کند.

مورد کاربرد: خروج از سیستم *پایاچک*

این مورد کاربرد نیز همچون مورد کاربرد ورود، به خودی خود یک مورد کاربرد نیست، اما در مورد کاربردهایی که در فوق ذکر شد، استفاده می‌شود.

پایاکاربر، خروج از سیستم پایاچک را انتخاب می‌کند. سیستم، جلسهٔ پایاکاربر را خاتمه می‌دهد.

نمودارهای توالی سیستم *پایاچک*

در این بخش، طراحی نمودارهای توالی، برای موارد کاربرد سیستم پایاچک که در بخش ٤-١-١ تشریح گردیدند، ارایه می‌گردد در نمودارهای توالی، خطوط عمودی برای نشان دادن خط زندگی کنشگر و سیستم استفاده می‌شود، و جهت کمان‌ها، جهت تعامل را نشان می‌دهد. اگر یک مورد کاربرد دارای چندین جریان باشد، چندین دیاگرام توالی نیاز خواهد داشت.

نمودار توالی صدور کارت‌امضای‌پایا

مطابق توضیحات بخش ٤-١-١-١ و شکل ٤-١، با توجه به دو مورد کاربرد برای صدور به صورت مراجعه حضوری و اینترنتی، دو نمودار توالی برای صدور کارت امضای پایا در شکل ٤-٢ و ٤-٣ آورده شده است. در موردی که منع قانونی برای تمدید گواهی امضا وجود داشته باشد، در هر یک از این دو نمودار توالی، با اعلام به ذی‌نفع، توالی پایان می‌یابد.

نمودار توالی صدور دسته‌چک‌پایا

این نمودار نیز مشابه نمودار توالی صدور کارت‌امضای‌پایا و مطابق توضیحات بخش ٤-١-١-٢ و شکل ٤-١، با توجه به دو مورد کاربرد برای صدور به صورت مراجعه حضوری و اینترنتی، دو نمودار توالی برای صدور دسته‌چک‌پایا در شکل ٤-٤ و ٤-٥ آورده شده است. در موردی که منع قانونی برای تمدید گواهی امضا وجود داشته باشد، در هر یک از این دو نمودار توالی، با اعلام به ذی‌نفع، توالی پایان می‌یابد.

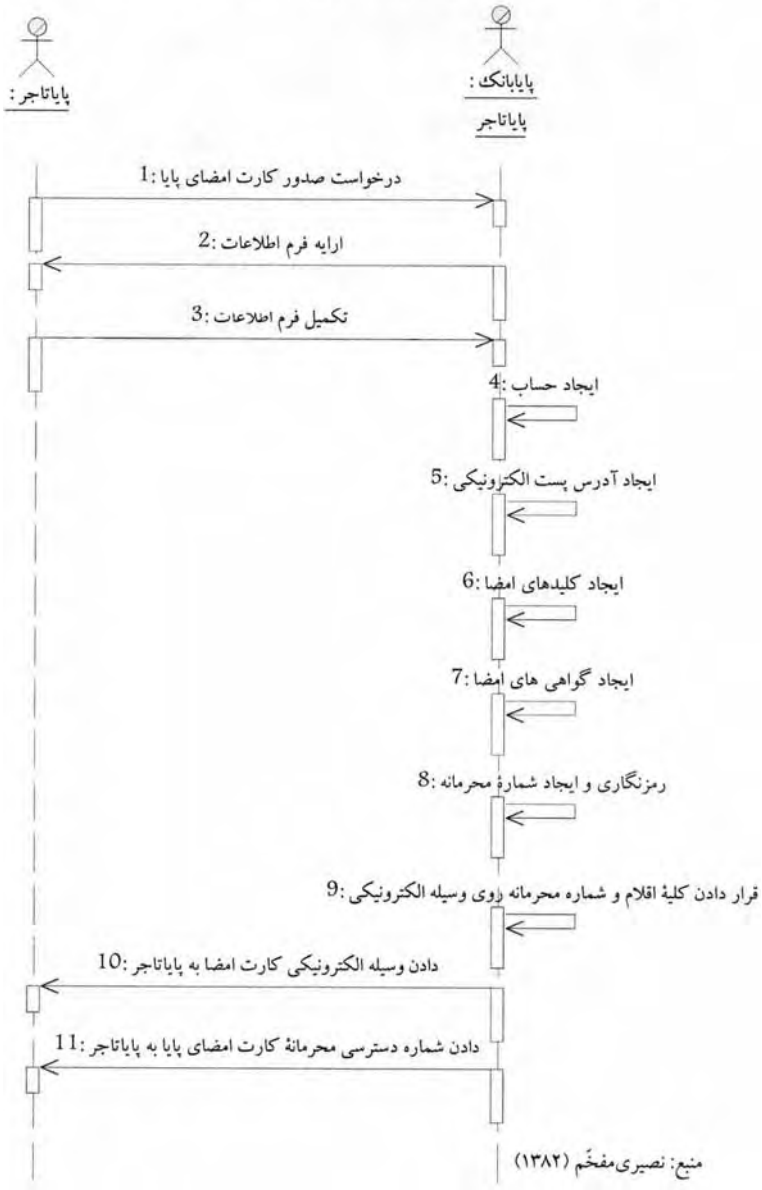
نمودار توالی صدور کارت‌امضای‌پایا/دسته‌چک‌پایا در پایابانک

این نمودار، در واقع مراحل ٤ تا ٩ در شکل ٤-٢، و مراحل ٥ تا ١٠ در شکل ٤-٤ است، که بین اجزاء داخلی یک پایابانک برقرار است.

نمودار توالی صدور و امضای پایاچک برای خرید در پایابنگاه

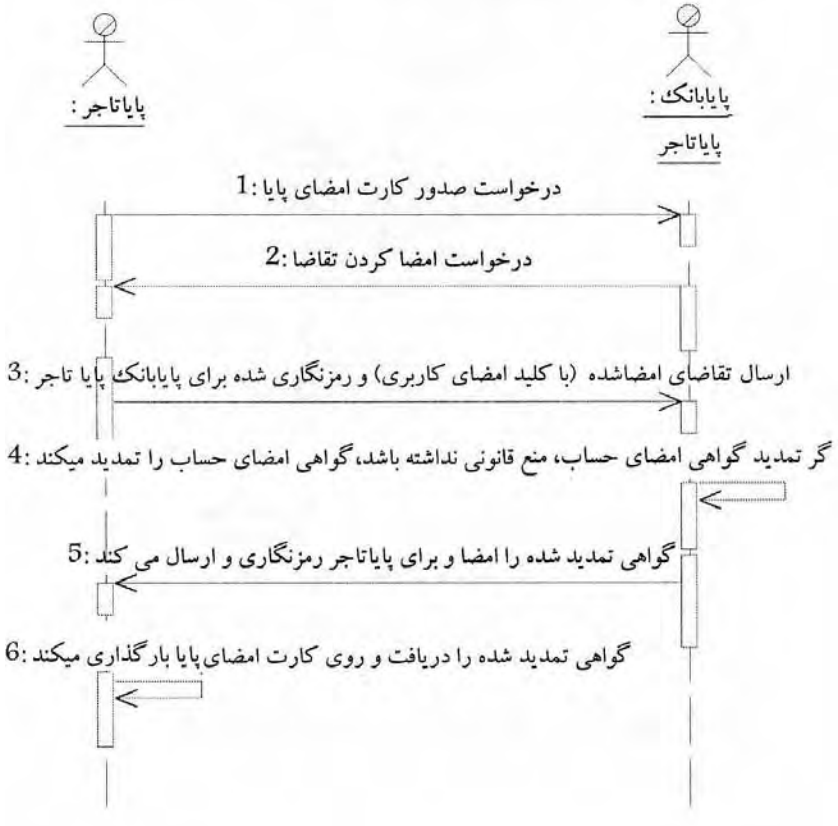
همانگونه که در بخش ٤-١-١-٤ آمده است و شکل ٤-١ نیز نشان می‌دهد، پایاتاجر به ازای درخواست امضاشده‌ای که پایامشتری برای کالای مورد نظرش بر روی پایابنگاه قرار داده است، صورت‌حساب امضاشده‌ای به او ارسال می‌کند. سپس پایامشتری پس از ورود به سیستم پایاچک، برای صدور پایاچک، مراحل را طی می‌کند که در شکل ٤-٦ آمده است.

شکل ۴-۲- نمودار توالی صدور حضوری کارت امضای پایا



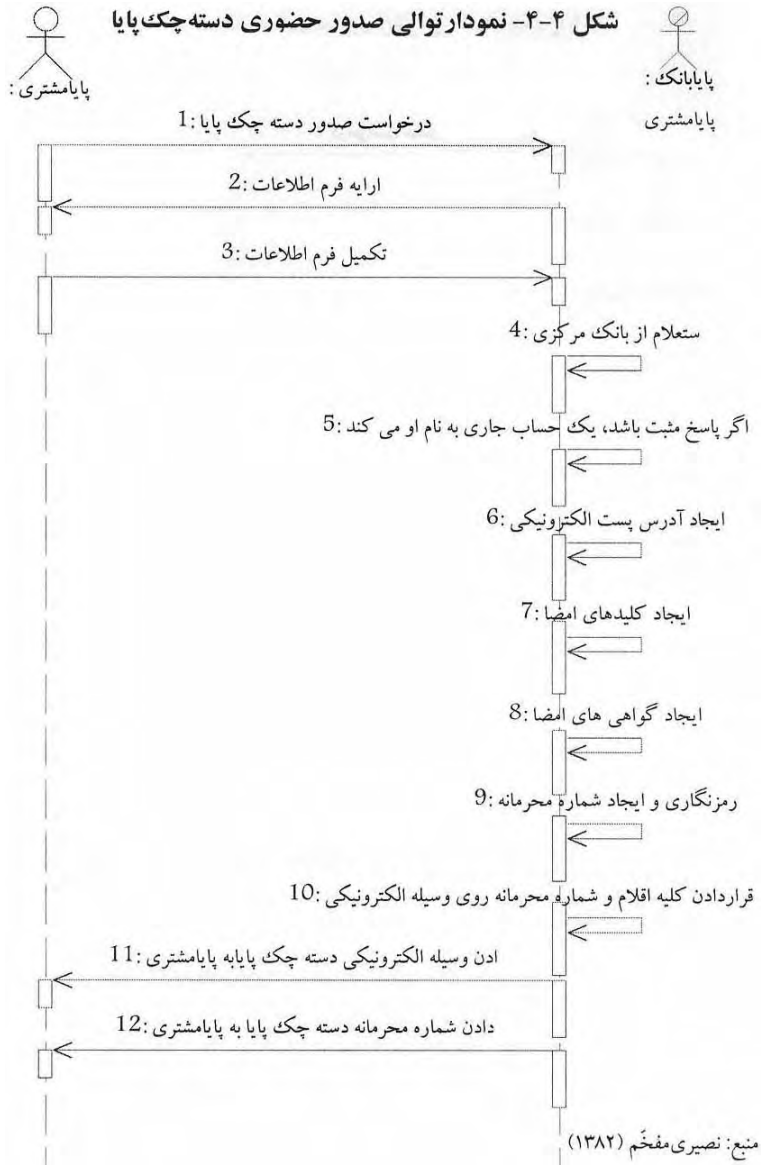
منبع: نصیری‌مفخّم (۱۳۸۲)

شکل ۴-۳- نمودار توالی صدور اینترنتی کارت امضای پایا



منبع: نصیری‌مفخّم (۱۳۸۲)

شکل ۴-۴- نمودار توالی صدور حضوری دسته‌چک پایا



منبع: نصیری‌مفخَم (۱۳۸۲)

شکل ۴-۵- نمودار توالی صدور اینترنتی دسته‌چک پایا

منبع: نصیری‌مفخّم (۱۳۸۲)

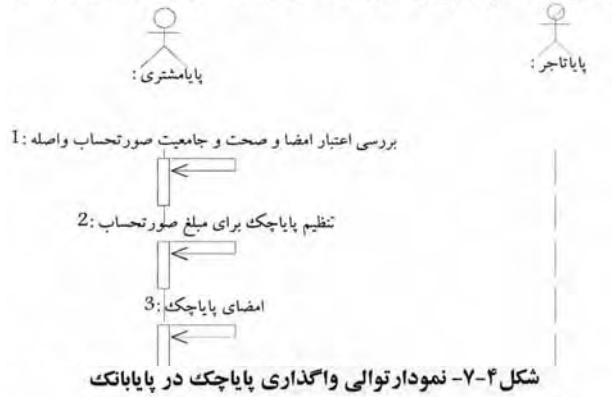
نمودار توالی واگذاری پایاچک در پایابانک

پایاتاجر پس از بررسی صحت صورت‌حساب و پایاچک، پایاچک را امضا و به پایابانک خود واگذار می‌کند. مطابق بخش ٤-١-١-٥ و شکل ٤-١، نمودار توالی واگذاری پایاچک به صورت شکل ٤-٧ آمده است.

نمودار توالی پرداخت پایاچک در پایابانک

ایـن نمـودار توالی مربوط به شبکهٔ بین بانکی است. همانگونه که در بخش ٤-١-١-٦ و شـکل ٤-١ آمده است، دو مورد کاربرد برای هنگامی که پایابانک پایامـشتری و پایابانک پایاتاجر، یکسان یا متمایز باشند، وجود دارد. در هردوی ایـن مـوارد کاربرد، چنانچه پایاچک پایامشتری برگشت بخورد، اگر پایامشتری عـضو مؤسـسهٔ عامـل باشـد و از اعتبار مناسب برخوردار باشد، پایاچک او از طـرف مؤسـسهٔ عامـل پـرداخت می‌گردد. نمودار توالی برای مورد کاربردی که پایاچک روی حساب پایامشتری برگشت بخورد، ولی پایامشتری عضو مؤسسهٔ عامل بوده و اعتبار کافی داشته باشد، در شکل ٤-٨ آمده است.

شکل ۴-۶- نمودار توالی صدور و امضای پایاچک برای خرید در پایابنگاه

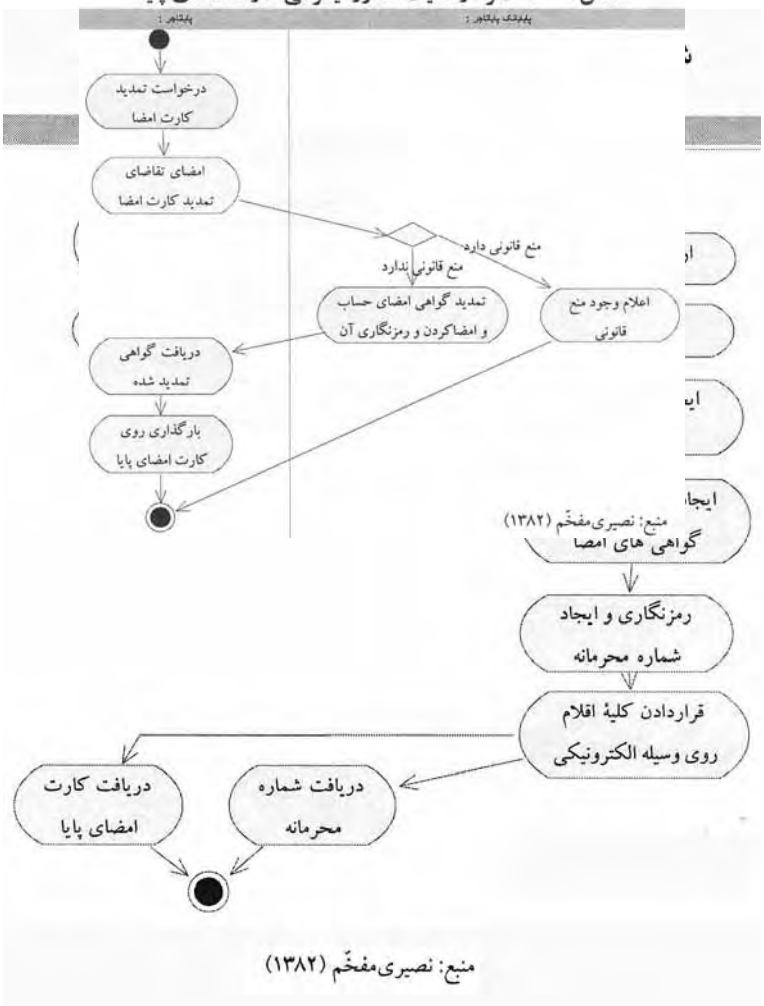


شکل ۴-۷- نمودار توالی واگذاری پایاچک در پایابانک

نمودارهای فعالیت سیستم پایاچک

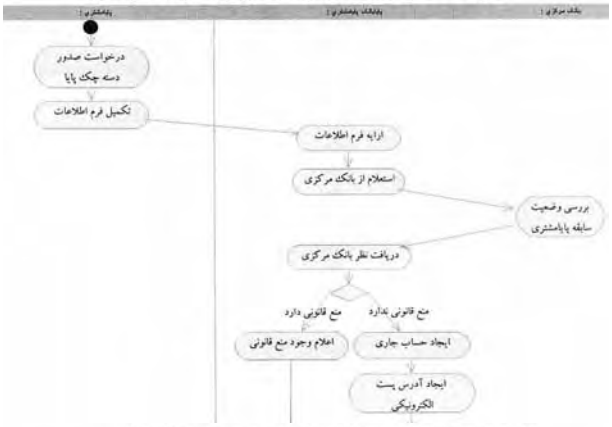
در این بخش، طراحی نمودارهای فعالیت را برای موارد کاربرد سیستم پایاچک که در بخش ٤-١-١ تشریح گردیدند، ارایه می‌دهیم. نمودار، فعالیت جریان کنترل از یک فعالیت به دیگری را در طول اجرای مورد کاربرد نشان می‌دهد. فعالیت‌ها با مستطیلی گرد گوشه نشان داده شده است. با پایان یک فعالیت، اجرا به حالت بعدی می‌رود. خطوط عمودی بیانگر مرز کنش‌گرهای درون سیستم هستند.

شکل ۴-۱۰- نمودارفعالیت صدور اینترنتی کارت امضای پایا



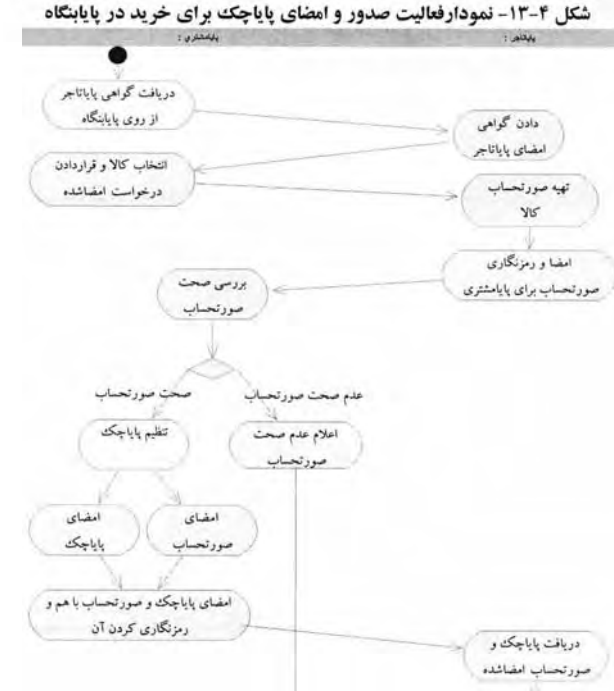
منبع: نصیری‌مفخّم (۱۳۸۲)

شکل ۴-۱۱- نمودارفعالیت درخواست حضوری صدور دسته چک پایا

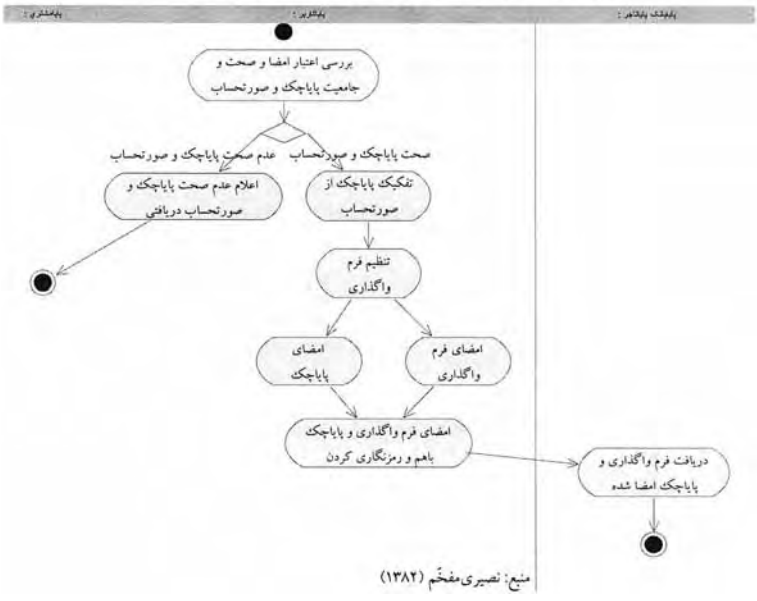


شکل ۴-۱۲- نمودارفعالیت درخواست اینترنتی صدور دسته چک پایا

شکل ۴-۱۳- نمودارفعالیت صدور و امضای پایاچک برای خرید در پایابنگاه



شکل ۴-۱۴- نمودارفعالیت واگذاری پایاچک در پایابانک



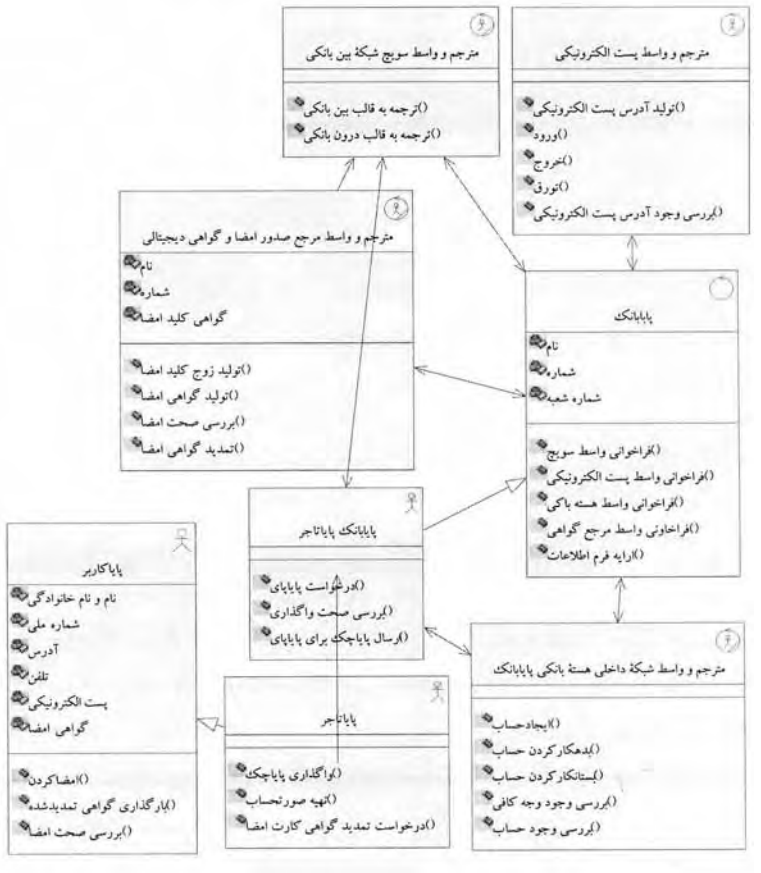
منبع: نصیری‌مفخّم (۱۳۸۲)

نمودار کلاس سیستم پایاچک

نمودار کلاس، مهم‌ترین نمودار در روش‌های شیءگراست و انواع اشیاء داخل سیستم و انواع مختلف ارتباطات استاتیکی آنها را نشان می‌دهد.

کلاس‌های پایه‌ای که در سیستم پایاچک مورد استفاده قرار می‌گیرند، فوق‌کلاس‌های پایاکاربر و پایابانک هستند. پایاتاجر و پایامشتری، زیرکلاس‌های فوق‌کلاس پایاکاربر، و پایابانک تاجر و پایابانک مشترک، زیرکلاس‌های فوق‌کلاس پایابانک هستند. روی تمامی سندهای دیجیتالی اعم از صورت‌حساب، پایاچک، و فرم واگذاری و حتی دستور پرداخت از طرف مؤسسهٔ عامل به پایابانک پایامشتری، امضاکردن و رمزنگاری با کلید عمومی طرف مقابل انجام می‌شود. لذا فوق‌کلاسی نیز بنام سند دیجیتالی داریم که این کلاس‌ها، زیرکلاسِ آن هستند.

شکل ۴-۱۵- نمودار کلاس صدور اینترنتی کارت امضای پایا



منبع: نصیری‌مفخّم (۱۳۸۲)

نمودار کلاس صدور اینترنتی کارت امضای پایا

بـر اسـاس نمـودار توالـی صدور اینترنتی کارت امضای پایا در شکل ٤-۳، نمودار کلاس آن به صورت شکل ٤-۱۵ آمده است.

نمودار کلاس صدور اینترنتی دسته چک پایا

بـر اسـاس نمـودار توالـی صـدور اینترنتـی دسته چک پایا در شکل ٤-٥، نمودار کلاس آن به صورت شکل ٤-١٦ آمده است.

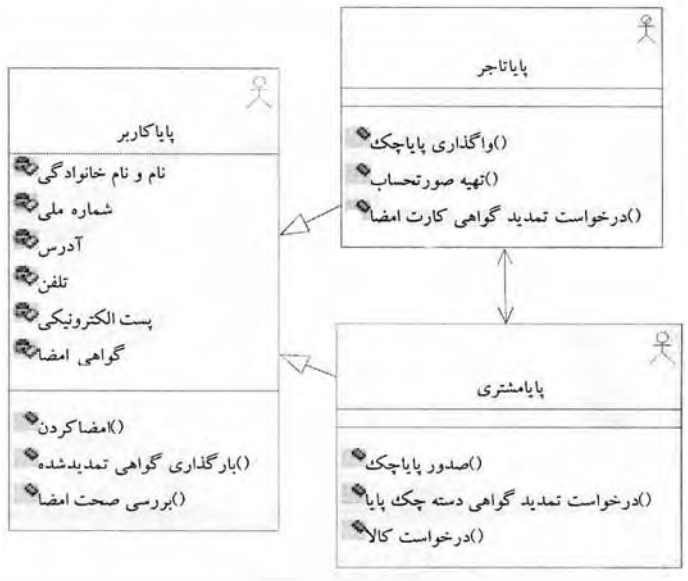
شکل ۴-۱۶- نمودار کلاس صدور اینترنتی دسته‌چک پایا

منبع: نصیری‌مفخّم (۱۳۸۲)

نمودار کلاس صدور پایاچک برای خرید در پایابنگاه

بر اساس نمودار توالی صدور پایاچک برای خرید در پایابنگاه در شکل ٤-٦، نمودار کلاس آن به صورت شکل ٤- ١٧ آمده است.

شکل ۴-۱۷- نمودار کلاس صدور پایاچک برای خرید در پایابنگاه



منبع: نصیری‌مفخّم (۱۳۸۲)

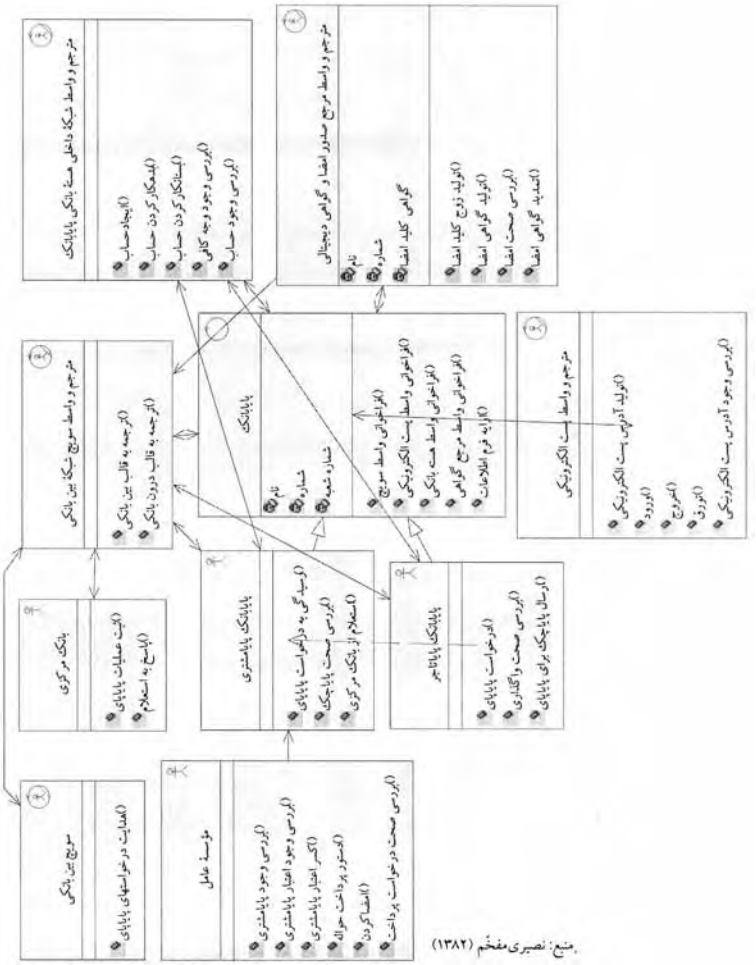
نمودار کلاس واگذاری پایاچک در پایابانک

بر اساس نمودار توالی واگذاری پایاچک در پایابانک در شکل ٤-٧، نمودارهای کلاس که حاوی پایاتاجر و پایابانک پایاتاجر و فوق‌کلاسهای آنها است، دقیقاً مشابه شکل ٤-١٥ است که از تکرار آن پرهیز می‌شود.

نمودار کلاس پرداخت پایاچک در پایابانک

بر اساس نمودار توالی پرداخت پایاچک در پایابانک در شکل ٤-٨، نمودارهای کلاس آن به صورت شکل ٤-١٨ آمده است.

شکل ۴-۱۸- نمودارهای کلاس پرداخت پایاچک در پایابانک



منبع: نصیری‌مفخم (۱۳۸۲)

پیاده‌سازی مدل سیستم *پایاچک*

در بخش ٤-١ طراحی مفاهیم و سناریوهای مدل سیستم پایاچک که در فصل سوم پیشنهاد شد، تحت UML ارایه گردید. مدل سیستم پایاچک کاملاً عام و مستقل از نوع نرم‌افزار یا سخت‌افزار و محیط مورد استفاده است و قابل

پیاده‌سازی روی وب، دستگاه‌های خودپرداز، دستگاه‌های با پروتکل WAP[۱]، و دستگاه‌های با کارت PCMCIA می‌باشد. مدل سیستم پیشنهادی پایاچک، در کمیته تحقیقاتی گروه کاربران ایرانی سوئیفت[۲] پذیرفته شده است و توسط J۲EE[۳] و XML[٤] در دست پیاده‌سازی عملی است. J۲EE و XML، به ترتیب فراهم‌کنندهٔ کدها و داده‌های قابل حمل[٥] هستند .

J۲EE و XML، با تجمیع با یکدیگر، ویژگی سازگاری[٦] را که برای استفاده در محیط‌های تجارت الکترونیکی، به دلیل گستردگی دامنهٔ فراجغرافیایی کاربران و کاربردها ضروری است، فراهم می‌آورند. قابلیت‌های امنیتی درون‌ساخت J۲EE نیز همراه با سازگاری و قابلیت حمل، آن را انتخاب شایسته‌ای برای محیط‌های تجارت الکترونیکی با امنیت بالا، همچون پرداخت‌های الکترونیکی می‌نماید (بامبارا، ۲۰۰۲؛ داکتا، ۲۰۰۰؛ داربی، ۲۰۰۱؛ دیتل، ۲۰۰۱؛ گالبریث، ۲۰۰۲).

در راستای این تحقیق، مطالعه‌ای نیز در مورد ebXML[۷] (ای‌بی‌ایکس‌ام‌ال، ۲۰۰۵؛ نصیری‌مفخّم و همکاران، شهریور ۱۳۸۱) صورت گرفت، که به عنوان استانداردی برای تسهیل و توسعهٔ بالقوهٔ کاربردهای تجارت الکترونیکی برای SMEها مطرح است؛ ولی چون در طول این تحقیق، فاز نهایی این استاندارد هنوز به پایان نرسیده بود، لذا به استفاده از XML بسنده شد.

در سیستم‌های پرداخت الکترونیکی، امنیت جایگاه ویژه‌ای دارد، که مراحل آزمون و استقرار پیاده‌سازی واقعی مدل، نیازمند حضور مرجع صدور گواهی است که با تدوین نظام ملی تایید هویت (CA[۸] & PKI[۹]) و امضای دیجیتالی و نهاد مدیریت کلان آن، توسط دبیرخانه شورای عالی اطلاع‌رسانی

---

۱. **Wireless Application Protocol**

۲ ـ جلسات این کمیته که یکی از زیر مجموعه‌های گروه کاربران ایرانی سوئیفت است، به ریاست آقای افشین کیانی، در محل بانک مرکزی جمهوری ایران تشکیل می‌گردد. این کمیته از بانک‌های دولتی و خصوصی جمهوری اسلامی ایران و کمیته ارتقای فرهنگ بانکداری الکترونیکی، کمیته دلفی (گروه مشورتی) سیستم پایاچک بوده است.

۳. **Java 2 Enterprise Edition**

٤. **eXtensible Markup Language**

٥. **Portable**

٦. **Interoperability**

۷. **electronic business XML**

۸. **Certificate Authority**

۹. **Public Key Infrastructure**

و وزارتخانه‌ها و دستگاه‌های همکار، و طراحی، تدوین و پیاده‌سازی بانکداری الکترونیکی، توسط وزارت امور اقتصادی و بانک‌ها و شرکت‌های مخابرات، امکان‌پذیر خواهد بود (سازمان مدیریت و برنامه‌ریزی کشور، ۱۳۸۱-۱-۲). امید آن داشتیم که در طول این تحقیق بتوانیم از PKI و CA ایران استفاده نماییم، اما رایزنی‌های آن در کشور انجام شده است و مرجع عالی صدور گواهی ایران، طی سال آینده قابل دسترسی خواهد بود. همچنین برای پیاده‌سازی واقعی این مدل، به طوری که دربردارندهٔ کلیهٔ موارد پیشنهادی مدل سیستم پایاچک باشد، سرورهای توانمندی همچون IBM WebSphere و Jakarta Tomcat برای بکارگیری J۲EE به همراه یک سرور پست الکترونیکی و Oracle برای پایگاه داده موردنیاز، مناسب هستند که برای این تحقیق دانشگاهی، از نظر محدودیت زمانی و هزینه، استفاده از آنها میسر نبود. اما در نمونه‌سازی تحقیقاتی برای پیاده‌سازی این سیستم، از Microsoft .NET استفاده گردید.

در بخش ٤-۲-۱، برخی از موارد پیاده‌سازی عملی سیستم پایاچک تحت J۲EE و یک نمونه‌سازی از آن در .NET ارایه می‌شود.

مواردی از پیاده‌سازی عملی و شبیه‌سازی سیستم پایاچک

JSP (Java Server Pages)، Servelet و Enterprise Beans از قابلیتهای J۲EE نسبت به نسخهٔ عادی J۲SE[1] است. JSP و Servelet برای صفحات دینامیکی یا استاتیکی XML و HTML استفاده می‌شوند. JavaBeanها جریان داده را بین سرور و کاربر مدیریت می‌کنند.

محصولات J۲EE لازم برای برآورده کردن نیازهای امنیتی و عملکرد مدل سیستم پایاچک، Java Mail API (JavaMail)، JavaBeans Architecture Framework API (JAF)، Java Cryptography Architecture (JCA)، Java Authentication & Authorization Service (JAAS)، Java Cryptography Extension (JCE)، و Java Secure Socket Extension (JSSE) هستند.

---

۱. Java 2 Standard Edition

JCA چهار بسته دارد. java.security برای بلوک‌های امنیتی مقدماتی JDK[1]، java.security.acl برای لیست‌های کنترل دسترسی، java.security.cert برای کلاس‌ها و واسط‌های گواهی X.۵۰۹، java.security.interfaces برای واسط‌های تولید و نمایش زوج کلیدهای RSA و DSA، و بالاخره، java.security.spec برای مشخصات پارامترها و کلیدهای الگوریتم‌ها هستند.

فراهم‌کنندهٔ این خدمات، الگوریتم‌های امضای دیجیتالی، الگوریتم‌های خلاصه پیام، الگوریتم‌های تولید کلید، تولید کنندهٔ کلیدها، مخزن کلیدها، تولیدکنندهٔ گواهی‌ها، و تولیدکنندهٔ اعداد تصادفی است؛ و برای مخفی نگه داشتن کلیدها در مخزن، آنها را با ویژگی opaque نگه می‌دارد.

همچنین با استفاده از بسته‌های .javax.mail ، برای ارسال یک نامه‌الکترونیکی، سه مرحلهٔ پیکربندی یک جلسه برای برنامهٔ کاربردی، تشکیل یک پیام، و ارسال آن باید انجام شود. در پیوست پنجم از (نصیری‌مفخّم، ۱۳۸۲) برخی از کدهای J۲EE مربوط به رمزنگاری، امضاها و گواهی، و ارسال و دریافت نامه‌ای همراه با الصاق از روی یک سرور پست الکترونیکی سیستم درحال پیاده‌سازی عملی پایاچک آمده است.

در نمونه‌سازی تحقیقاتی از پیاده‌سازی عملی سیستم پایاچک، از Microsoft .NET استفاده گردید و از آنجا که قالب سند پایاچک به صورت XML در نظر گرفته شده است، برای پایگاه داده نیز از XML DataBase استفاده شده است. همانگونه که در فصل سوم و بخش ٤-١ دیدیم، موجودیت‌های این سیستم از نوع پایامشتری، پایاتاجر، و پایابانک هستند. کاربر با login در سیستم، براساس شناخت شناسه و رمزعبور کاربری مبنی بر اطلاعات ثبت شده از پایاکاربر، براساس نقش او که پایامشتری یا پایاتاجر است، به صفحهٔ مربوطه هدایت می‌گردد. خدمات در دسترس برای پایا مشتری، عبارت از مشاهده صورت‌حساب‌های وارده، صدور پایاچک، مشاهدهٔ لیست پایاچک‌های صادره و تمدید دسته‌چک‌پایا است. پایامشتری، با انتخاب گزینهٔ صدور پایاچک، برای صورتحساب واردهٔ انتخابی که مبلغ و پایاتاجر مربوط به آن متناظراً استخراج و بر روی فرم پایاچک حاوی اطلاعات

---

۱. java development kit

مربوط به حساب و پایابانک خود او نمایش داده شده، پایاچک را امضا و به پایاتاجر ارسال می‌کند. تاریخ از روی سرور بانک کنترل می‌شود و لذا چک‌ها دقیقاً به همان تاریخ تنظیم آنها، صادر می‌شوند. پایامشتری می‌تواند لیست پایاچک‌هایی را که برای پایاتاجران صادر نموده، مشاهده کند. متقابلاً پایاتاجر می‌تواند لیست پایاچک‌های وارده را مشاهده کرده و پایاچکی را برای مرحلهٔ واگذاری به پایابانک خود انتخاب کند. پایاتاجر نیز می‌تواند لیست پایاچک‌های واگذارشده را مشاهده نماید و یا پایاکارت خود را تمدید کند. پیاده سازی این گزینه‌ها براساس پروتکل‌های فصل سوم (بخش ۳-۲-۷) و طراحی آنها در فصل چهارم (بخش ٤-۱) است.

فصل پنجم:
نتیجه‌گیری، پیشنهادات و راهکارهای آینده

تحـول سیـستم‌هـای پـرداخت، از جملهٔ مهم‌ترین ملزومات برای پیوستن ایران به صـحنهٔ تجـارت الکترونیکـی اسـت. با توجه به وسعت استفاده از چک در معاملات تجـاری در ایـران، در ایـن نوشتار، مدل پایاچک را برای سیستم چک الکترونیکی در ایـران ارایـه نمـودیم. طراحـی این مدل بر اساس قانون چک جمهوری اسلامی ایران، امکانـات موجـود در شـبکه اینترنت و استانداردهای پرداخت، زیرساختارها، امکانات نظام‌های پرداخت کشور و نیازها صورت گرفته است.

سـاختار فعلـی نظـام بانکـداری در ایـران فاقد سیستم پایاپای و تسویه مکانیزه بین بانکـی بـرای چـک‌هـا اسـت، ولی با سیستم پیشنهادی پایاچک، سند دیجیتالی چک که حـاوی دسـتور پرداخت است، از روی اینترنت بین پایابانک‌های مربوطه مبادله می‌شود. بـا اتکـا بـه مـرجع تأیـید گواهـی‌ها و امضاهای دیجیتالی، امکان بررسی صحت سند و هـویت موجودیت‌های دخیل در جریان پرداخت در نزد هرکدام ازموجودیت‌ها، از روی اینتـرنت میسر است. سپس پایابانک پایامشتری، در صورت وجود وجه کافی در حساب پایامـشتری، پـس از بدهکارکردن حَساب او، از طریق پیامی با پایابانک پایاتاجر، پایاپای و تـسویه مـی‌کـند. ایـن پایابانک نیز پس از بستانکارکردن حساب پایاَتاجر، نتیجه را به وی اعلام می‌کند.

سیستم پایاچک، ضمن برخورداری از سهولت پرداخت چک الکترونیکی روی اینترنت و امکان بررسی سریع موجود بودن وجه، این امکان را فراهم می‌سازد که مشتریان بر اساس درجه‌ای از اعتبارشان، از طرف شرکت ثالثی موسوم به مؤسسهٔ عامل، چک برگشتی‌شان پرداخت شود، و درعوض، متحمل درصد هزینهٔ بیشتری برای پردازش چک‌های آتی‌شان باشند. چنانچه شرکت ثالث، چک برگشتی آنها را پرداخت نکند، در اینصورت، برگشتی بودن پایاچک به پایابانک پایامشتری و نهایتاً به پایابانک پایاتاجر و شخص پایاتاجر و خود پایامشتری اعلام می‌گردد. بدین طریق، ضمن حفظ اسرار مالی پایامشتریان، امکان پرداخت شدن پایاچک‌های پایامشتریان خوش اعتبار که به دلایل اشتباهاتی برگشت خورده است فراهم می‌گردد. به منظور پایاپای نقدی پایابانک‌های پایامشتری و پایاتاجر، از «شتاب» استفاده می‌شود. از طرفی، با محقق شدن سیستم تسویه ناخالص بلادرنگ(RTGS)، پایابانک‌هایی که سپرده‌شان در بانک مرکزی، کمتر از مبلغ پایاچک وارده برای تسویه باشد، قادر به تسویهٔ پایاچک پایامشتری خود نخواهند بود، و از اینرو پایابانک‌ها نیز برای پائین نگه داشتن

درصد پایاچک‌های برگشتی خود، نسبت به حفظ سپردهٔ مناسب در بانک مرکزی از طریق مدیریت نقدینگی مبادرت خواهند کرد.

همچنین با قرار دادن یک زوج کلید اضافه به عنوان «کلیدامضای‌کاربری»، یک پایاکاربر می‌تواند روی یک کارت، دارای یک امضای کاربری و چندین امضای حساب باشد و هرکدام از حساب‌ها که سربیاید، شمارهٔ کاربری او در بانک محفوظ است. مدل سیستم پایاچک، مدلی عام است و می‌توان آن را روی دستگاه‌های خودپرداز، دستگاه‌های با پروتکل WAP و دستگاه‌های با کارت PCMCIA نیز پیاده‌سازی نمود.

ارزیابی سیستم پایاچک

در فصل سوم دیدیم که FSTC eCheck و MANDATE از سیستم‌های چک‌الکترونیکی برای ردهٔ پرداخت‌های کلان الکترونیکی هستند که به مراحل عملیاتی یا نمونهٔ عملیاتی رسیده‌اند. همانگونه که در فصل سوم نیز بیان گردید، سیستم MANDATE تشابه بسیاری با سیستم FSTC eCheck دارد، ولی از آنجا که مدل FSTC در فاز جلوتری نسبت به MANDATE است[1]، سیستم پایاچک را با FSTC eCheck مقایسه می‌نماییم.

در سیستم پایاچک، همانگونه که در ابتدای بخش نیز ذکر گردید، علاوه بر «زوج کلید امضای حساب» یک زوج کلید اضافه به عنوان «کلید امضای کاربری[2]» در کارت در نظر گرفته شده است و این امکان در هیچ یک از دو سیستم FSTC eCheck و MANDATE، پوشش داده نشده بود.

در قسمت ارتباط بین پایابانک پایامشتری و مؤسسهٔ عامل، مؤسسهٔ عامل دستور پرداخت از حساب او به حساب پایا مشتری را به پایابانک پایامشتری را می‌دهد. پس بدین صورت، مدل حوالهٔ الکترونیکی را هم علاوه بر چکِ الکترونیکی در این تحقیق پوشش داده‌ایم.

در فصل اول، ویژگی‌هایی را که یک سیستم پرداخت الکترونیکی باید دارا باشد، برشمردیم[3]. همانگونه که ملاحظه می‌شود، برخی از این ویژگی‌ها دارای وجوه اشتراک و برخی نتیجهٔ برخی دیگر هستند. لذا می‌توان این ویژگی‌ها را در گروه کوچکتری به صورت زیر طبقه‌بندی نمود.

۱. *امنیت:* جعل ناپذیری ابزار پرداخت
۲. *قابلیت اطمینان:* قابلیت دسترسی سیستم
۳. *مقیاس‌پذیری:* قابلیت تغییر اندازه سیستم بدون افت کارایی

---

۱ ـ FSTC eCheck و MANDATE در بخش ۲-٤ مقایسه شده است.
۲ـ بخش ۳-۲-۲ را ببینید.
۳ ـ فصل ۱، بخش ۱-۲.

٤. *اعتماد:* درجهٔ اختفای پول و اطلاعات افراد در سیستم
٥. *قابلیت تبدیل:* قابلیت تبدیل ارزها و مکانیزم‌های متفاوت پرداخت
٦. *کارایی:* توانایی انجام پرداخت‌های خرد بدون افت کارایی
۷. *سادگی استفاده:* سادگی خرید و انجام خودکار مکانیزم پرداخت بدون ورود به جزئیات پیچیده
۸. *نوع مجوز:* انجام پرداخت با/ بدون اتصال بلادرنگ با مرجع مرکزی
۹. *قابلیت انتقال:* پرداخت بدون دخالت شخص ثالث (بانک)
۱۰. *کاربست‌پذیری:* سطح بکارگیری ابزار پرداخت
۱۱. *سازگاری:* براساس استانداردهای باز و بدون وابستگی به سازمانی خاص

از این میان نیز، ویژگی‌هایی که مستقیماً توسط کاربر قابل شهود است، امنیت، قابلیت اطمینان، اعتماد، قابلیت تبدیل، کارایی، سادگی استفاده، قابلیت انتقال و کاربست‌پذیری هستند. به دلیل اینکه افراد می‌توانند به سادگی نسخه مجددی از داده‌ها را در کامپیوتر خود تولید کنند، بدون دخالت شخص ثالث برای تصدیق در ضمن فرایند پرداخت، اجتناب از پرداخت وجوه جعلی، غیرممکن می‌شود. لذا تاکنون امکان پیاده‌سازی ویژگی قابلیت انتقال در سیستم‌های پرداخت الکترونیکی محقق نگردیده است[1]. از آنجائیکه در نظرگرفتن همهٔ این ویژگی‌ها، پیاده‌سازی سیستم‌های پرداخت الکترونیکی را دشوار می‌نماید، معمولاً زیرمجموعه‌ای از آنها را مورد توجه قرار می‌دهند. اما در ارزیابی عملی یک سیستم پرداخت الکترونیکی، پارامترها از چندین جنبهٔ تکنیکی، اقتصادی، اجتماعی و قانونی ملاک عمل قرار می‌گیرند.

در **جنبهٔ تکنیکی،** امنیت مورد توجه‌ترین برای شرکت‌ها و مصرف‌کنندگان است که ملزومات آن بدین شرح است:

- *مجازبودن*: تأیید شناسه‌های همهٔ طرف‌های دخیل و جلوگیری از اشخاص ثالث از تخریب اطلاعات یا انتقال دادن غیر مجاز
- *محرمانگی*: حفظ اطلاعات گسیل شده و ممانعت از دسترسی اشخاص غیر مجاز به اطلاعات محرمانه
- *جامعیت*: جلوگیری از تراکنش‌های دست‌کاری شده و اجتناب از ارسال دوباره
- *نفی انکار*: مصرف‌کننده و تولیدکننده در صورت مشارکت، نتوانند مشارکت‌شان را در تراکنش انکار کنند. رکوردهای جزئیات و زمان و اطلاعات مربوطه در پایگاه داده امنی نگهداری شود.

---

۱ ـ ادعا می‌شود که Mondex تنها ابزار پرداخت است که قابلیت انتقال دارد به (نصیری‌مفخّم، ۱۳۸۲، فصل ۲) مراجعه کنید.

جنبهٔ اقتصادی مرتبط با ارزش ارز واقعی و مرتبط با درجهٔ گستردگی استفاده از اینترنت است و پارامترهای مطرح در آن چنین هستند:

- *هزینهٔ تراکنش‌ها*: هزینه‌های مستقیم یا غیرمستقیم پرداخت شده توسط خریدار و فروشندهٔ دخیل در تراکنش، برای انتخاب در سیستم‌های پرداخت کوچک، عامل تصمیم‌گیرنده است.
- *مبادلهٔ تفکیک ناپذیر*: یعنی در *طی تراکنش*، مشتری پول یا چیزی با ارزش معادل می‌پردازد.
- *دامنهٔ کاربر*: دامنه‌ای از کاربران که سیستم پرداخت الکترونیکی برای آنها قابل دسترس است. آیا سیستم در تمام کشورهای دنیا و برای همهٔ سنین قابل دسترس است؟
- *جابجایی ارزش*[1]: روش، محدود به شرکتی که ارزش را تولید کرده نباشد و در مکان‌های متفاوتی یا با ارزش معادلی استفاده شود.
- *خطر مالی*: درجه امنیت تراکنش‌های online

جنبهٔ اجتماعی یک سیستم آن است که، اگر جامعه باید به آن اعتماد کرده و از آن استفاده کند، باید به نیازهای اجتماعی اشاره کند، که عبارتند از:

- حفظ محرمانگی مشتری از اینکه *رد اطلاعاتش* گرفته شود
- *درجهٔ مقبولیت*: باید ساده و کاربرپسند باشد، بخصوص برای پرداخت‌های کوچک
- *جابجایی پذیری*: کاربران الزام نداشته باشند که همیشه از همان کامپیوتر برای دسترسی به اینترنت استفاده کنند. بخصوص ذخیره روش‌های پرداختی روی سخت‌افزار کامپیوترهای در مکان‌های چند کاربره، نامعقول و غیر عملی است، و باید از همه جا قابل دسترس باشد.

جنبهٔ قانونی اشاره به مواردی اینچنین دارد:

- باید *منطبق بر قوانین و مقررات دولتی* باشد: امضاهای دیجیتالی، انتقال‌های دیجیتالی و قانونی بودن پرداخت‌ها، قراردادهای الکترونیکی، استانداردهای تکنیکی، جمع‌آوری مالیات‌های اجاره‌ای تراکنش‌های بین‌المللی
- باید *نظیر سیاست‌های منطقه‌ای و کشوری* باشد.

بر اساس این پارامترها ارزیابی مدل پایاچک را به همراه ارزیابی چک الکترونیکی FSTC، در جدول ۵-۱ شرح داده شده است. این جدول نشان می‌دهد که در مدل پایاچک، علاوه بر مزیت وجود زوج «کلید امضای کاربری»، که به یک پایاکاربر، این امکان را می‌دهد که روی یک کارت، دارای یک امضای کاربری و چندین امضای حساب باشد و هرکدام از حساب‌ها که سربیاید، شمارهٔ کاربری او در بانک محفوظ

---

۱. **Value mobility**

جدول ۵-۱-ارزیابی سیستم چک الکترونیکی FSTC و سیستم پیشنهادی پایاچک
(تعداد علامتهای کنار هر ویژگی، میزان برآوردن ویژگی مربوطه را نشان می‌دهد)

ویژگیها		FSTC eCheck		سیستم پیشنهادی پایاچک
مجاز بودن	☑☑☑	از امضاهای دیجیتالی و گواهی‌های دیجیتالی برای بررسی شناسه استفاده می‌کند	☑☑☑	از امضاهای دیجیتالی و گواهی‌های دیجیتالی برای بررسی شناسه استفاده می‌کند
محرمانگی	☑☑	گرچه از کلیدهای طلایی نامتقارن برای محاسبه و ارسال اطلاعات استفاده می‌کند، اطلاعات حساب پرداخت مشتری در معرض خطر دزدیده شدن است	☑☑	گرچه از کلیدهای طلایی نامتقارن برای محاسبه و ارسال اطلاعات استفاده می‌کند، از آنجا که چک الکترونیکی در تطابق با قانون چک است و در آن ناشناس بودن مطرح نیست، با توجه به تعریف و ماهیت چک، پارامتر کلیدی نیست.
جامعیت	☑☑☑	برای اطمینان از جامعیت اطلاعات تراکنش، از شماره گواهی اطلاعات و کلیدهای طلایی نامتقارن برای امنیت افزون استفاده می‌کند	☑☑☑	برای اطمینان از جامعیت اطلاعات تراکنش، از شماره گواهی اطلاعات و کلیدهای طلایی نامتقارن برای امنیت افزون استفاده می‌کند
نفی انکار	☑☑☑	از امضاهای دیجیتالی و چک‌های دیجیتالی برای اطمینان از نفی انکار استفاده می‌کند	☑☑☑	از امضاهای دیجیتالی و چک‌های دیجیتالی برای اطمینان از نفی انکار استفاده می‌کند
توسیع	☑☑☑	دسته‌چک‌های الکترونیکی مصرف‌کننده و فروشگاه تراکنش را کامل می‌کنند. سیستم‌های مالی فقط گواهی چک و مبادلات را فراهم می‌کنند	☑☑☑	دسته‌چک‌های الکترونیکی مصرف‌کننده و فروشگاه تراکنش را کامل می‌کنند. سیستم‌های مالی فقط گواهی چک و مبادلات را فراهم می‌کنند
کارایی تراکنش	☑☑☑	اما اگر تراکنش offline باشد، کارایی تراکنش کاهش خواهد یافت	☑☑☑	ارتباط online برای بررسی اعتبار گواهی امضای طرف مقابل، ریسک را کمتر می‌کند. اما اگر تراکنش offline باشد، کارایی تراکنش کاهش خواهد یافت.
تطابق	☑☑☑	مطابق با یک حساب واقعی و سازمان‌های مالی ستی است	☑☑☑	مطابق با یک حساب واقعی و سازمان‌های مالی ستی است
مقبولیت	☑	شرکت و مشتریان هردو باید دستگاه کارت خوان (برای خواندن کارت هوشمند) نصب کنند	☑☑	شرکت و مشتریان هردو باید دستگاه کارت خوان (برای خواندن کارت هوشمند) نصب کنند. همچنین با استفاده از فلاپی، بدون نیاز به کارت خوان، با امکان استفاده از اینترنت از هر کامپیوتری، مقبولیت بیشتری دارند.

باشد، وجود مؤسسهٔ عامل، باعث بهبود نقدینگی حساب پایامشتریان می‌شود. همچنین از جدول ۵-۱ مشاهده می‌شود که سیستم نمونهٔ پایاچک از نظر هزینهٔ تراکنش، تفکیک‌ناپذیری مبادله، دامنهٔ کاربران، و جابجایی‌پذیری، بر سیستم FSTC eCheck برتری دارد. گرچه پیاده‌سازی عملی این سیستم با بکارگیری امکانات کارت‌های هوشمند خواهد بود که از نظر مجازبودن، محرمانگی، جامعیت و نفی انکار نیز تأمین باشد، ولی در نمونه‌سازی آن با فلاپی دیسک، این ویژگی‌ها کمرنگ‌تر خواهد بود.

جدول ۵-۱- ادامه

ویژگیها		FSTC eCheck		سیستم پیشنهادی پایاچک
هزینه تراکنش		هزینه تراکنش‌های عادی پایین است، اما باید جوابگوی دسته‌چک‌های الکترونیکی (کارت‌های هوشمند) و گواهی‌های دیجیتالی و دیگر هزینه‌های ثابت باشد		هزینه تراکنش‌های عادی پایین است، ولی هزینه‌های ثابت برای گواهی‌ها و امضاها برقرار است (دستگاه کارت‌خوان و کارت‌های هوشمند دسته‌چک‌های الکترونیکی)
مبادلهٔ تفکیک ناپذیر		اول از چک استفاده می‌شود، بعداً پرداخت می‌شود	☑☑	با توجه به قانون چک ایران، برای صدور به تاریخ پرداخت، در حالی که هر دو در یک بانک حساب داشته باشند، بصورت pay now است و مورد علاقهٔ فروشندگان.
دامنهٔ کاربر	☑☑	محدود به آنهایی است که یک حساب جاری دارند	☑☑☑	چون می خواهیم مطابق قانون چک عمل کنیم. ولی با صدور کارت‌هایی برای دارندگان حساب‌های پس انداز، به آنها نیز امکان وصول و واگذاری چک به حساب‌شان (و نه امکان صدور چک) را می‌دهیم.
جابجایی ارزش	☑☑☑	از محدودهٔ پشت‌نویسی استفاده می‌شود. می‌تواند بین طرف‌ها منتقل شود	☑☑☑	از محدودهٔ پشت‌نویسی استفاده می‌شود. می‌تواند بین طرف‌ها منتقل شود
خطر مالی	☑☑	مصرف‌کنندگان می‌توانند پرداخت‌های چک را برای تراکنش‌های مسئله‌دار متوقف کنند	☑☑	چون قانون چک توقف پرداخت را منع کرده مگر با ادلهٔ قانونی و این موضوع خارج از محیط الکترونیکی فعلی است، امکان دستور توقف پرداخت و درخواست لغو گواهی‌ها بدلیل مفقود شدن دسته چک یا PIN، بررسی‌های حقوقی بیشتری را می‌طلبد.
ناشناسی		هر کسی که چکی را می‌نویسد و منتقل می‌کند، لازم است نامش را امضا کند		هر کسی که چکی را می‌نویسد و منتقل می‌کند، لازم است نامش را امضا کند
راحتی	☑☑	لازم است مصرف‌کنندگان برای یک دسته‌چک الکترونیکی از یک بانک اقدام کنند	☑☑	لازم است مصرف‌کنندگان برای یک دسته‌چک الکترونیکی از یک بانک اقدام کنند و با درخواست صدور الکترونیکی، راحت‌تر می‌شود
جابجایی	☑☑☑	شامل امضا کردن، گواهی کردن، امضای چک‌های جاری محلی، بررسی قانونی بودن و یکتایی چک	☑☑☑	شامل امضا کردن، گواهی کردن، امضای چک‌های جاری محلی، بررسی قانونی بودن و یکتایی چک، و با دسترسی به اینترنت از روی هر کامپیوتری mobility بهتر می‌شود.

در جدول ۵-۲، با توجه به قانون چک و کاستی‌های آن که در فصل سوم مورد نقد و بررسی قرار گرفت و راهکارهایی پیشنهاد شد، با توجه به نیازهای پوشش داده نشده توسط سیستم چک سنتی که با سیستم پایاچک، امکان اجرای آنها فراهم می‌گردد، مقایسه‌ای بین سیستم پایاچک و سیستم چک سنتی به عمل آمده است.

جدول ۵-۲- ارزیابی سیستم پایاچک و سیستم چک سنتی (با توجه به موارد قانون چک و کاستی‌های آن)

مشکل سیستم چک سنتی	راه حل سیستم پایاچک
ممانعت از صدور چک‌های وعده‌دار (مشروط) و سفید امضا امکان ندارد	موقع نوشتن چک، تابع مربوطه از صدور چک بی مبلغ (سفید امضا) جلوگیری می کند
در کمتر مواردی، مطابقت کارشناسانه امضای روی چک با امضای صاحب حساب صورت می‌گیرد	با امضاهای دیجیتالی در تک تک موارد این امر بررسی و صحت‌سنجی دقیق می‌شود
در سیستم بانکی سنتی هیچ اثری از ظهرنویس در اطلاعات بانکی ثبت نمی‌شود و زمینه انتقال به افراد مجعول و پول‌شویی فراهم است	واسطه مالی بین صادرکننده، وصول‌کننده و ظهرنویسان به وضوح قید و ثبت می‌شود. همچنین امکان صدور چک حامل و حذف رد پاها برداشته می‌شود.
در مورد حساب‌های دولتی، به گواهی امضا، قبل از رسیدن چک نیاز است، که بر خلاف این بخشنامه، بانک‌ها آن را در اتاق پایاپای در فرصت کوتاه ارایه می‌دهند که مجالی برای بررسی صحت آن نیست	گواهی دیجیتالی امضاها، همیشه همراه امضاهای روی چک است.
روشی در دست نیست که فرد برای دریافت چک از اعتبار صادرکنندهٔ آن آگاه باشد که بداند که چک را بپذیرد یا خیر (نبود اطلاعات کافی در مورد "میزان بی‌اعتباری" صادر کنندگان قبل از قبولی چک از آنها)	در مورد چک‌های متعلق به شعب یک بانک، موجودی بلافاصله online بررسی و اعلام می‌شود و در این موارد، تاجر پس از کسب تأیید پرداخت، کالا را می‌تواند بفرستد. در مورد پایاچک‌های متعلق به پایابانک دیگر نیز پس از کسب اطلاع از وضعیت موجودی از طریق اینترنت و سویچ بین بانکی (با اتصال با بانک اطلاعاتی چک‌های برگشتی در بانک مرکزی)، تاجر می‌تواند نسبت به قبول پایاچک اقدام کند. در سایر موارد، با حمایت مؤسسهٔ عامل در کنار پایابانک پایامشتری احتمال برگشت خوردن پایاچک‌های پایامشتریان کمتر می‌شود.
عدم ایجاد رد پای چک	با log کردن رکورد چک، از صدور، واگذاری و پرداخت در سمت تمامی طرف‌های دخیل، رد آن و جزئیات آن درج می‌شود و غیر قابل انکار است
صورت‌حساب چک‌های کارسازی‌شده حداقل یک‌بار در سال به سپرده‌گذار ارسال می‌شود	با هر پرداخت صورت‌حساب پرداخت‌شدن آن چک، بلافاصله به مشتری داده می‌شود و در صورت جعل نیز، صاحب حساب در اسرع وقت از بروز جرم مطلع می گردد
-	با تبدیل پیام‌ها به SWIFT در محل سرور بانک، قادر به ارسال پیام‌های بین المللی با ارزهای مختلف خواهیم بود.

ادامه جدول در صفحه بعد

جدول ۵-۲- ادامه

مشکل سیستم چک سنتی	راه حل سیستم پایاچک
شروط و مد امضا (چند امضایی) تا موقع رسیدن چک به بانک مشتری قابل بررسی نیست	شروط لازم برای محدودهٔ مبلغ چک برای حساب خاص و مد امضای آن در کارت موجود بوده و موقع صدور، کنترل می‌شود و می‌توان کنترل کرد که چک‌های دولتی از حساب‌های خاص، غیر قابل انتقال باشد.
هزینه تحویل و پست چک‌ها و صورت‌حساب‌ها	حذف هزینه تحویل و پست چک‌ها و صورتحساب‌ها (بهبود مدیریت نقدینگی)
عدم امکان دسترسی سریع به تمامی داده ها	دسترسی سریع به داده‌ها (بهبود مدیریت نقدینگی)
مصرف کاغذ، سوخت (حمل و نقل)، ...	کمک به حفظ محیط زیست
ریسک مالی درصورت جعلی بودن چک‌ها و امضاها باعث عدم اعتماد به وصول چک از هر فرد است.	به لطف گواهی‌ها و امضاهای دیجیتالی، اکثر تراکنش‌ها بدون ریسک مالی برای پرداخت‌کننده، دریافت‌کننده یا سیستم بانکی است و باعث اعتماد مردم و حفظ نقش بانک‌ها در نظام نقدینگی می‌شود.
ریسک مالی درصورت جعلی بودن چک‌ها و امضاها	اصلی یا جعلی بودن چک‌ها به سادگی قابل بررسی است. (گواهی‌ها همراه اطلاعات صاحب حساب و دسته چک و کلید عمومی ذخیره شده‌اند)
پرداخت‌کننده مجاز بودنش را با امضای هر چک بیان می‌کند	علاوه بر آن، امضاهای دیجیتالی اثبات می‌کنند که فقط خود آن پرداخت‌کننده سفارش آن پرداخت را داده است، چون او فقط کلید خصوصی امضا را دارد و نه هیچ فرد دیگری (نفی انکار)
لزوم مراجعه فیزیکی به شعبه‌ای از بانک مشتری برای هر چک	مراجعه فیزیکی فقط برای اثبات هویت واقعی جهت افتتاح حساب چک الکترونیکی و صدور اولین دسته چک لازم است. بانک‌ها قادر به جمع آوری الکترونیکی واگذاری‌ها به حساب‌های کاربران می‌شوند.
بررسی امضای پرداخت‌کننده فقط در بانک پرداخت‌کننده، و آن هم فقط به صورت نادر مورد بررسی کارشناسان امضا (در صورت مورد قضایی) قرار می‌گیرد.	استفاده از گواهی‌های کلید عمومی، هویت‌شناسی پایاچک را توسط دریافت‌کننده، و بانک‌های دریافت‌کننده و پرداخت‌کننده امکان‌پذیر می‌سازد و امضاهای دیجیتالی می‌توانند به طور خودکار، اعتبارسنجی شوند.
روی چک‌های کاغذی فقط نام دریافت‌کننده ذکر می‌شود که می‌تواند مجعول باشد و باظهرنویسی، به شخص ثالثی منتقل شود و نیز اگر گم شود، هر کسی با آن نام می‌تواند از آن استفاده کند.	در حالیکه در محیط الکترونیکی وقتی با کلید عمومی آن دریافت‌کنندهٔ خاص رمز شود، فقط خود او می‌تواند از آن استفاده کند و نه هیچ کس دیگری
در چکهای کاغذی، هزینه پردازش بر عهدهٔ دریافت‌کننده است	دو طرف می‌توانند در طی مذاکره روی مبلغ و تاریخ و ...، توافق کنند که هزینه پردازش به عهدهٔ پرداخت‌کننده، یا دریافت‌کننده یا هر دو (هر کدام هزینه‌های در سمت خود) باشد و از حساب کسر شود، و این در متن پیام‌های سوئیفتی تعبیه شده است.
در چک‌های کاغذی از شعبی از یک بانک، پایاپای در استان مربوطه و سپس در مرکز، و سپس در اتاق پایاپای کل انجام می‌شود	هر دو بانک می‌توانند مقادیر پایاپای را به‌طور دو طرفه online منتقل کنند، نیازی به خدمات پایاپای متمرکز نیست و فقط باید با پایابانکهای دیگر پایاپای نماید.

پیشنهادها و راهکارهای آینده

با توجه به بکارگیری کارت هوشمند با قابلیت پردازش‌های چندگانه (کارت چندمنظوره)، با فراخوانی رویه‌های امنیتی متفاوتی از روی آن کارت، می‌توان از خدمات پایاچک، پول الکترونیکی و کارت اعتباری بر روی یک کارت استفاده نمود. علاوه بر پیاده‌سازی سیستم چک الکترونیکی روی دستگاه‌های خودپرداز، می‌توان با پیاده‌سازی آن روی دستگاه‌های دارای پروتکل WAP، کامپیوترهای کیفی، Palm و

PDA بـا کـارت PCMCIA نیـز، بـه طور مجازی بانک را در هر لحظه و هر جا با افـراد همـراه نمـود و از جایگـاه واقعـی چک در تثبیت نظام نقدینگی سود جست. با اسـتفاده از تلفـن‌هـای همـراه، بـا قابلـیت خواندن کارت‌های هوشمند، بدین طریق با اسـتفاده از پروتکل‌های مربوطه، به معنای کامل می‌توان یک بانک جیبی و نسل بعدی چکهـای الکترونیکـی، یعنـی m-Check[1] را داشـت. در آیـنده‌ای نزدیک، با خودکار شـدن عملیات پایاپای بین بانکی در ایران، الحاق سیستم پرداخت چک الکترونیکی با اتاق پایاپای خودکار به عنوان نقطهٔ عطف روشنی بین سیستم‌های پرداخت الکترونیکی و بانکداری الکترونیکی خواهد بود.

در زمیـنه هوش مصنوعی، با الهام از مدل SafeCheck می‌توان هم از عامل‌های متحـرک هوشـمند استفاده نمود و هم اینکه پایگاه‌های دادهٔ مورد جستجو را به موتور استنتاج مجهز نمود. کار روی قواعد پایگاه دانش مورد استفاده برای مؤسسهٔ عامل، در تـصمیم‌گیری برای میزان اعتبار افراد مهم است. همچنین شبکه‌های عصبی نیز در این گونه تصمیم‌گیری‌ها می‌تواند استفاده شود.

ایـن گـونه اسـتنتاج‌ها می‌تواند در پایگاه دانشی در شبکه‌ای دیگر در مورد ارجاع چـک الکترونیکـی بـه همـراه یـک دادخواست الکترونیکی (که با استخراج از قوانین موجود در پایگاه تنظیم شده)، به دادگاه الکترونیکی تنظیم شود و در آنجا نیز بر اساس استنتاج‌های موجود در پایگاه دانش، استدلال و تصمیم‌گیری شود و به عبارتی، توسط قواعد تصمیم‌گیری در پایگاه دانش، می‌توان قضاوت الکترونیکی و وکالت الکترونیکی داشـت. بازار بورس اسناد الکترونیکی از دیگر مواردی است که با الهام از ویژگی‌های همه‌جانبهٔ سیستم چک الکترونیکی، برای سایر اسناد می‌تواند بسط یابد.

از موضوعاتی که در مسیر این تحقیق، بررسی نمودیم، زبان ebXML بود که به عـنوان استانداردی برای تسهیل و توسعهٔ کاربردهای تجارت الکترونیکی برای SME ها مطرح است، ولی چون در طول این تحقیق، فاز نهایی آن هنوز به پایان نرسیده بود [۱۴۳،۳۱]، لـذا بـه اسـتفاده از XML در شـبیه‌سـازی *پایاچک* بسنده کردیم. شایسته اسـت که مکانیزم‌های قوی امنیتی که FSTC در FSML به کار گرفت، برای اعمال و استفاده در ebXML مورد بررسی قرار گیرند.

با توجه به تعاریف و نیازهای ارایه شده در فصل سوم و نظر به رفع مشکلات مطرح در استفاده از چک در سیستم پرداخت، در راستای این تحقیق، پیش‌نویس اولیه‌ای از قانون چک الکترونیکی برگرفته از قانون تجارت و قانون چک تهیه نمودیم. جدا از آنکه ارایه قانون جامعی برای چک الکترونیکی، کاملاً خارج از حوزهٔ این

---

۱. **Mobile Check**

نوشتار است، از یک طرف، تنظیم چنین قانونی، همفکری حقوق‌دانان و قانون‌گذاران و کلیهٔ صاحبان علم و فن در این زمینه را می‌طلبد، و از طرف دیگر، چون قانون چک کاغذی به مرور برگرفته از نیازهای فرهنگی جامعه بوده است و ازآنجائی‌که چک الکترونیکی ابزاری جدید در نظام پرداخت است و فرهنگ خاص آن باید بوجود آید، این قانون نمی‌تواند منحصراً حاصل فکر حقوق‌دانان باشد و بایستی با بررسی‌های اصولی تنظیم گردد. با توجه به قانون تجارت الکترونیکی جمهوری اسلامی ایران و نیز با بررسی مفادی از قانون تجارت در مورد برات که برای چک نیز کاربرد دارند، و با توجه به قانون چک الکترونیکی که در FSTC eCheck اشاره گردیده است، می‌توان قانون جامع و مانعی برای چک الکترونیکی تنظیم نمود. تنظیم چنین قانونی برای چک الکترونیکی به عنوان ابزاری جدید در نظام پرداخت، هم‌فکری حقوق‌دانان و قانون‌گذاران و کلیهٔ صاحبان علم و فن در این زمینه را می‌طلبد.

منابع

منابع انگلیسی

►►1.Abrazhevich, D. (2001), “Classification and Characteristics of Electronic Payment Systems”, EC-Web 2001, Springer-Verlag LNCS 2115, pp. 81-90.

►►2.Abrazhevich, D. (2001), "A Survey of User Attitudes towards Electronic Payment Systems", IPO, Center for User-System Interaction, Technical University of Eindhoven (TUE), Available at http://www.ipo.tue.nl/homepages/dabrazhe/ps/Library/data/hciihm2001sign.pdf, visited at 2003.

►►3.Abrazhevich, D. (2001), "Electronic Payment Systems: Issues of User Acceptance", ECWEB2001, Technical University of Eindhoven (TUE). Available at http://www.ipo.tue.nl/homepages/dabrazhe/ps/Library/data/ebiz2001.PDF, e2001_presentation.ppt, visited at 2003.

►►4.Ahmed, K. Z. and C. E. Umrysh (2002), *Developing Enterprise Java Applications with J2EE and UML*, Addison Wesley.

►►5.Anderson, M. M. (1998), "The Electronic Check Architecture", Version 1.0.2, September 29, Available at http://www.echeck.org/library/wp/ArchitecturalOverview.pdf, http://echeckworldwide.com/partnerdocs/eCheckOverview15.pdf, visited at 2003.

►►6.Anderson, M. M. (1999), "Echeck Tutorial", FSTC’s 1999 Fall General Meeting, September 22, Available at http://www.echeck.org/demos/meeting92299/EcheckTutorialMMA.zip, http://www.echeck.org/demos/meeting92299/EcheckTutorialMMA.pdf, visited at 2003.

►►7.Anderson et al. (2000), "Method And System for Processing Electronic Documents, US 6,021,202", United States Patent, Feb. 1, Available at http://www.echeckworldwide.com/pubdocs/US06021202.pdf, visited at 2003.

►►8.Anderson et al. (2001), "Method And System for Processing Electronic Documents, US 6,209,095 B1", United States Patent, Mar. 27,

►►9.Available at http://www.echeckworldwide.com/pubdocs/US06209095.pdf, visited at 2003.

►►10.Asokan, N., P.A. Janson, M. Teiner and M. Waidner (1999), "State of the Art in Electronic Payment Systems", October 4, Available at http://citeseer.nj.nec.com/cache/papers/cs/14830/http:zSzzSzwww.semper.orgzSzsirenezSzpeoplezSzasokanzSzresearchzSzac.pdf/asokan99state.pdf, visited at 2003.

►►11.AZS Services2002 (2003), "ISO-8583 SDK documentation and description", Version 1.51, Apr 24th, Available at http://www.a2zz.com, visited at 2003.

►►12.Bambara, J.J. and P R. Allen (2002), *J2EE UNLEASHED*, SAMS Publishing.

►►13.Braynov, S. (2001), "Introduction to Electronic Payment Systems", September 12, Available at http://www.cs.buffalo.edu/~sbraynov/e-commerce/lectures/lecture7_pdf.pdf, visited at 2003.

►►14.Central Bank of the Islamic Republic of Iran (2002), *Bulletin*, Vol. 41, Numbers 179-180, p. 22, Spring & Summer 1380 (2001/02), Avaliable at.http://www.cbi.ir/publication/PDF/bulletin179180.pdf, visited at 2003..

►►15.Chan, H., R. Lee, T. Dillon and E.Chang (2001), "*E-Commerce Fundamentals and Application"*, John Wiley & Sons Ltd.

►►16.Chaum, D. and S. Brands (1997), "Minting Electronic Cash", IEEE SPECTRUM, pp. 30-34, February.

►►17.Cleassens, J. et. al (2001), "On the Security of Today's Online Electronic Banking System", Computers and Security, 27 December, available at http://www.esat.kuleuven.ac.be/~joclaess/pub/stoebs.pdf, visited at 2003.

►►18.CommerceNet (2005), http://www.commerce.net.

►►19.CRIPTOMATHIC (2003), "Cryptomatic Certification Authority", CRIPTOMAThIC Technical White Paper, Version 1.0, 03.07.2003, Denmark, http://www.cryptomathic.com, visited at 2003.

►►20.Daconta, M. C. and A. Saganich (2000), "XML Development with Java 2", Sams Publishing.

►►21.Dani, A.R. and P.R. Krishna (2001), "An E-check Framework for Electronic Payment Systems in the Web Based Environment", EC-Web 2001, Springer-Verlag LNCS 2115, pp. 91-100.

►►22.Darbay, C., J. Griffin and P. de Haan (2001), *Java Networking*, Wrox press Ltd..

►►23.Deitel, H. M., P. J. Deitel and T. R. Nieto (2001), *e-Business & e-Commerce – How to Program*, Prentice-Hall.

►►24.Doggett et al. (1997), "Electronic Funds Transfer Instruments, US 5,677,955", United States Patent, Oct. 14, Available at http://www.echeckworldwide.com/pubdocs/US05677955.pdf, visited at 2003.

►►25.ebXML (2005), http://www.ebXML.org.

►►26.eCheck (2005), http://www.echeck.org.

►►27.eCheck Worldwide (2001), "Just4Dental Payment Pilot", Briefing Paper, 12/6/2001, Available at http://www.echeckworldwide.com/pubdocs/J4DeCheckBriefing .pdf, visited at 2003.
►►28.eCheck Worldwide Ltd. (2001), "eCheck Worldwide Announces the Completion of the Pilot Project outside of United States", 12 November, Available at http:// URL: http://www.echeckworldwide.com/press20011112.htm, visited at 2003.
►►29.eCheck Worldwide Ltd. (2001), "eCheque Worldwide Transaction Technology to eCommerce Landscape", 20 November, Available at http://www.echeckworldwide.com/press20011120.htm, visited at 2003..
►►30.eCheck Worldwide (2002), "Your eCommerce World just became real …", Available at http:// fstc-uvx.org/ 2002.07.30_UVX_Lessons_Learned_From_eCheck.ppt, visited at 2003.
►►31.eCheck Worldwide Ltd. (2002), "CommerceNet Announces Pilot Launching eCheck Australia", 20 September, Available at http://www.echeckworldwide.com/press20010920.htm, visited at 2003.
►►32.eCheck Worldwide (2005), http://www.echeckworldwide.com.
►►33.Ferreira, L.C. and R. Dahab (1998), "A scheme for Analyzing Electronic Payment Systems", IEEE, pp. 137-146.
►►34.Fowler, M. (2000), *UML Distilled*, Second Edition, Addison Wesley.
►►35.FSTC (2005), http://www.fstc.org.
►►36.FSTC Electronic Check project team (1999), *FSML: Financial Services Markup Language*, Version 1.50, July 14, available at http://xml.coverpages.org/fsml.html, http://www.echeck.org/library/ref/fsml15-brief.html, and http://www.echeck.org/library/ref/fsml20-logging.html, visited at 2003.
►►37.Galbreath, N. (2002), Cryptography for Internet and Database Applications, Wiley Publishing, Inc..
►►38.Gelinas, U. J. and J. L. Gogan (2001), "The FSTC Electronic Check Project", AICPA Case Development Program No. 96-10, March, Available at http://www.aicpa.org/download/edu/96-10a.pdf, visited at 2003.
►►39.Gradkell Systems Inc. (1999), "Using Public-Key Digital Signatures in Paperless Information Systems", GSA ADP Conference, May, Available at http://www.gradkell.com/PKI/dbsign-overview.pdf, visited at 2003.

►►40.Grant, N. (2000), "POP, RCK, ART, POD – The Exploding World of Electronic Checks", NACHA, November, Available at http:// ecc.nacha.org/resources/1100_World_of_Elec_Chks.ppt, visited at 2003.

►►41.Grigg, I. (2000), Security in 7 Layers, Springer-Verlag *Lecture Notes in Computer Science-1962*, 4th International Financial Cryptography Conference Proceedings, Anguilla, British West Indies, pp. 332-348, February.

►►42.Hamafekri (2005), http://www.hamafekri.org.

►►43.Hancock, D. and D. B. Humphery (1998), "Payment Transactions, Instruments, and Systems: A Survey", Journal of Banking & Finance, 21, pp. 1573-1624.

►►44.Heider, F. P., H. Nilson and D. Pinkas (1999), "Evaluation of the European Trusted Services Programme", ETS, April 6, Available at ftp://ftp.cordis.lu/pub/infosec/docs/etseg-finalrepo2.doc visited at 2003.

►►45.Hwang, M-S, I.C. Lin and L.H. Li (2001), "A Simple Micro-Payment", The Journal of Systems and Software 55, 221-229.

►►46.IRANAFACT (2005), http://www.iranafact.org

►►47.Iran Trade Point (2005), http://www.irtp.com.

►►48.Jaffe, F. (1998), "eCheck Overview", June 23, Available at http://www.echeck.org/demos/pdf/analyst4.pdf, visited at 2003.

►►49.Kelly, E.W.J. (1997), "Future of Electronic Money: a regulator's Perspective", IEEE SPECTRUM, pp. 20-22, February.

►►50.Khiaonarong, T. (2000), "Electronic Payment Systems Development in Thailand, International Journal of Information Management, 20, pp. 59-72.

►►51.Lee, J.K. and H. S. Yoon (2000), "An Intelligent Agents-Based Virtually Defaultless Check System: The SafeCheck System", International Journal of Electronic Commerce, Vol. 4, No. 3, pp. 87-106, Spring, Available at http://kgsmweb.kaist.ac.kr/re_center/paper/2000-097.pdf, visited at 2003.

►►52.Mandate II Consortium (1998), Mandate Final Report, Draft Version 2.0, 24/2/98, Available at: http://mandate2-final-report.doc, visited at 2003.

►►53.MARINADE LTD (1999?), MANDATE FUNCTIONAL REQUIREMENTS, Available at http://www.cryptomathic.com/pdf/finalrep.pdf, visited at 2003.

►►54.Mittelholzer, T. and A. Mueller (1997), "New Payment Instrument Prototype", Deliverable D15, SEMPER Consortium, IBM France, December 10.

►►55.M'Raihi, D., M. Yung (2001), "E-Commerce applications of smart-cards", Computer Networks 36, 453-472.
►►56.Neuman, B. C. and G. Medvinsky (1995), "Requirements for Network Payment: The NetCheque Perspective", Proceedings of IEEE Compcon'95, San Francisco, March, Available at http://www.isi.edu/people/bcn/papers/pdf/9503_netcheque-neuman-medvinsky-compcon95.pdf, visited at 2003.
►►57.Schneir, B. (1994), *Applied Cryptography*, John Wiley & Sons Inc..
►►58.Schutze, S. (1999), "Electronic Check", Virtual Covernment'99, February 24, Available at http://www.echeck.org/library/presentations/virtual-gov99.pdf, visitred at 2003.
►►59.SET (2005), http://www.SET.com.
►►60.Shamos, M. I. (2002), "Electronic Payment Systems", Institute for eCommerce, Carnegie Mellon University, Fall 2002, Available at http://euro.ecom.cmu.edu/program/courses/tcr763/2002pgh/, visitred at 2003.
►►61.Shamos, M. I. (2002), "Electronic Payment Systems", Available at http://euro.ecom.cmu.edu/program/courses/tcr751/2002/, visitred at 2003.
►►62.Sherif, M. H. (2000), *Protocols for Secure Electronic Commerce*, CRC Press.
►►63.SHETAB (2005), http://www.shetab.org.
►►64.Sirbu, M. A. (1997), "Credit and Debits on the Internet", IEEE SPECTRUM, pp. 23-29, February.
►►65.SWIFT (2005), http://www.swift.com.
►►66.Tanenbaum, A. S. (2003), *Computer Networks*, Prentice-Hall Inc., 4rd Edition.
►►67.Triversity Product Development (2003), *Transnet Financial XML Message Specification (DRAFT)*, January 17.
►►68.Trusted Security Solutions (2000), "A98: ATM Initial Key Establishment System, ISO8583 message Format Specification", Version 1.4, May 2.
►►69.United Nations (2001), "E-Commerce and Development Report 2001,Chapter7- Management Payment and Credit Risks Online: New Challenges for Financial Service Providers", United Nations Conference on Trade and Development, New York and Geneva, Available at http://r0.unctad.org/ecommerce/event_docs/chapter7_ecom2001.pdf, visitred at 2003.
►►70.Wade, C. (1998), "Overview of Cryptography Used in the FSTC Treasury Electronic Checking Market Trial",

Available at http://www.echeck.com /echeck_security_Tut_pp97_w.ppt, visitred at 2003.

►►71.Wade, C. (1999), "eCheck: An overview and explanation of security measures", September 22, Available at http://www.echeck.org/demos/meeting92299/echeck-overview-security.pdf, visitred at 2003.

►►72.Wade, C. (2000), "Tutorial: Over the Internet Payments", CommerceNet 2000, October 29, Available at http://www.commerce.net/events/past/ppt/cn2000/SIPTutorial.ppt, visitred at 2003.

►►73.Weber R. (1998), "Technical Report TUM-I9819, Chablis - Market Analysis of Digital Payment Systems", Version 1.0, TU Munich, August 18th, Available at http://wwwbib.informatik.tu-muenchen.de/infberichte/1998/TUM-I9819.ps.gz, visitred at 2003.

►►74.Weber R. (2000), "Technical Report TUM-I9819, Chablis - Market Analysis of Digital Payment Systems", Compact Version 2.0, February 11, Available at http://graphics.tu-bs.de/v3d2/pubs/chablis-marketanalyse.pdf , visitred at 2003.

►►75.Weise, J. (2001), "Public Key Infrastructure Overview", Sun BluePrints OnlineSun microsystems, August, Available at http://www.sun.com/blueprints, visitred at 2003.

►►76.Ya, X.W., S.S. Yuan (2000?), "Account Based Secure Electronic Check", National University of Singapore, Acvailable at http://www.nus.edu.sg/~ssung/publications/1013.pdf, visitred at 2003.

►►77.Yu, H.C., K.H. His and Kou (2002), "Electronic Payment Systems: an analysis and comparison of types", Elsevier Science, Pergamon, Technology in Society 24, 331-347.

منابع فارسی

۱ـ آسیا (۱۳۸۲)، «چک الکترونیکی ایران طراحی شد». *روزنامه آسیا*، ۱۳۸۲/٤/۱۲، شماره ٤۱۸، ص. ۹، و نیز قابل دسترس در اخبار ایسنا، ۱۳۸۲/٤/۱۱، http://www.isnagency.com/news/NewsCont.asp?id=۲٤۸۵۰۲&lang=p، رویت شده در ۱۳۸۳.

۲ـ ابرار (۱۳۸۳)، «استفاده از چک الکترونیکی در نظام بانکی کشور امکان‌پذیر است». *روزنامه ابرار اقتصادی*، ۲۷ و ۱۳۸۳/٤/۲۸، شماره‌های ۱۷۳٤ و ۱۷۳۵، صص. ۱۸، و نیز قابل دسترس در گروه اخبار علمی ایرنا، ۱۳۸۳/٤/۲۳: http://www.irna.ir/?SAB=OK&LANG=PE&PART=_ARCHIVE&TYPE=_NARCHIVE&id=۱۳۸۳۰٤۲۳۱۰۳۷۵۷N۲۳ ، رویت شده در ۱۳۸۳.

۳ــ بانک ملت (۱۳۸۱)، «اصلاح قانون چک: ضرورت رد پای چک: نامه چک و اشکالات موجود در ایجاد ردپای قانونی»، قابل دسترس در http://www.hamafekri.org/dbase/upload/۳٤۹.pdf. رویت شده در ۱۳۸۲.

٤ــ بختیاری، شهرام (۱۳۸۱)، «بن دیجیتالی بر اساس ساختار رمز نامتقارن»، در مجموعه مقالات کنفرانس اروپایی آسیایی توسعه فناوری اطلاعات و ارتباطات و همایش بین‌المللی توسعه الکترونیک و فناوری اطلاعات استان فارس، دانشگاه شیراز، صص. ۱۸-۱۰، ۹-۷ آبان.

۵ــ پوررستم، قدیر (۱۳۸۱)، «مدل‌های اعتماد در بستر کلید عمومی»، در کتاب مقالات چهارمین همایش دانشجویی انجمن کامپیوتر ایران، دانشگاه آزاد اسلامی واحد نجف آباد، صص. ۳٦۹-۳٦۳، ۱٤-۱۲ شهریور.

٦ ـ حاجبی، سعید (۱۳۸۱)، «مقدمه‌ای بر پرداخت الکترونیکی»، قابل دسترس در http://www.iranweb.biz.com رویت شده در ۱۳۸۲.

۷ــ سازمان مدیریت و برنامه‌ریزی- دبیرخانه شورای عالی اطلاع‌رسانی (۱۳۸۱)، «طرح راهبردی: دولت الکترونیکی»، *روزنامه رسمی*، شماره ۱٦۷۱۳، ص. ۱٦، ٤/۲٦/ ۱۳۸۱.

۸ــ سازمان مدیریت و برنامه‌ریزی- دبیرخانه شورای عالی اطلاع‌رسانی (۱۳۸۱)، «طرح راهبردی: گسترش کاربرد فناوری ارتباطات و اطلاعات در اقتصاد، بازرگانی و تجارت»، *روزنامه رسمی*، شماره ۱٦۷۱۳، ص. ۱۸، ۱۳۸۱/٤/۲٦.

۹ـ ساعدی، مهدی (۱۳۷۹)، *چکیدهٔ UML*، شرکت توسعه نرم‌افزار هدا.

۱۰ــ عباسی، هادی (۱۳۸۱)، «بررسی مشکلات امنیتی رمزنگاری کلید عمومی در کارت هوشمند»، در مجموعه مقالات همایش بین‌المللی توسعه الکترونیک و فناوری اطلاعات استان فارس، صص. ٦٦-۵۹، ۹-۷ آبان.

۱۱ــ فانی، رضا (۱۳۸۰)، «اسکناس دیجیتال»، *منادی (نشریه علمی خبری انجمن رمز ایران)*، شماره ٦، صص. ۸-٦، اسفند.

۱۲ــ فرید، حمیرا و حشمی، علیرضا، (۱۳۸۰)، «آشنایی با مفاهیم تجارت الکترونیکی»، در مجموعه مقالات همایش جهانی شهرهای الکترونیکی و اینترنتی، جزیره کیش، صص ٤۳-٤۸، ۱۳-۱۱ اردیبهشت.

۱۳ـ«قانون چک»، قابل دسترس در http://www.sb۲٤.com/ib/cheque.doc رویت شده در ۱۳۸۲.

۱٤ـ کمیته تحقیقاتی گروه کاربران ایرانی سوئیفت (افشین کیانی،محمود ظهوریان، فاطمه حمیدی، زهرا سلطانی، فرزانه نقدی، شیوا متقی، فریا نصیری مفخّم) (۱۳۸۲)، «سیستم تسویه ناخالص آنی (RTGS)»، *جلد اول: مفاهیم وشناخت سیستم*، بانک مرکزی جمهوری اسلامی ایران، شهریور.

۱۵ــ کمیته ملی ادیفاکت ایران (۱۳۸۰)، «گزارش توجیهی و سیاست تجارت الکترونیکی جمهوری اسلامی ایران»، ویرایش ششم، پاییز ۱۳۸۰، قابل دسترس در http://www.iranafact.org/Seminar/fa/gozaresh.htm، رویت شده در ۱۳۸۲.

۱٦ـ کیانی، افشین (۱۳۸۱)، «گزارش بررسی چک در ایران»، مدیریت کل نظارت بر بانک‌ها و مؤسسات اعتباری، بانک مرکزی جمهوری اسلامی ایران.

۱۷ــ کیانی، افشین و حکیمی ناصر، (۱۳۸۱)، «پیش‌نویس مقررات حاکم بر مرکز شتاب»، مدیریت کل نظارت بر بانکها و مؤسسات اعتباری، بانک مرکزی جمهوری اسلامی ایران، نگارش ۱/۵، خرداد.

۱۸ــ مهدوی، فرج‌اله (۱۳۸۱)؛ «اصلاح قانون چک: مقالات و اظهار نظرها در مورد چک: چک و کاهش امکان جعل آن»، ۱۳۸۱/۳/۲۷، قابل دسترس در http://www.hamafekri.org/dbase/upload/faraj.pdf، رویت شده در ۱۳۸۲.

۱۹ــ هدوی، فرج‌اله (۱۳۸۱)؛ «اصلاح قانون چک: ضرورت رد پای چک: نامه آقای فرج اله مهدوی به وزیر اقتصاد در مورد ضرورت ردپای چک»، ۱۳۸۱/۳/۲۹، قابل دسترس در http://www.hamafekri.org/dbase/upload/۳٤۲.pdf، رویت شده در ۱۳۸۲.

۲۰ــ نبوی‌رضوی، سیدعلی‌اصغر (۱۳۷۰)، *بررسی قانون چک و نحوهٔ رسیدگی به شکایات چک بلامحل*، تهران، شرکت انتشارات جهان معاصر، بهار.

۲۱ــ نصیری‌مفخّم، فریا، «مقدمه‌ای بر تجارت الکترونیکی» (۱۳۸۰)، *دیتا (مجله تخصصی کامپیوتر دانشکده فنی دانشگاه اصفهان)*، شماره نهم، صص. ۵۳-۵۰، اسفند.

۲۲ــ نصیری مفخّم، فریا و محمدعلی نعمت‌بخش (۱۳۸۱)، «سازگاری ebXML در تجارت الکترونیکی»، در کتاب مقالات چهارمین همایش دانشجویی انجمن کامپیوتر ایران، دانشگاه آزاد اسلامی واحد نجف آباد، صص. ۲۳۱-۲۲٤، ۱٤-۱۲ شهریور.

۲۳ــ نصیری مفخّم، فریا ، محمدعلی نعمت‌بخش و احمد براآنی (۱۳۸۱)، «طراحی و مدل‌سازی یک سیستم چک الکترونیکی در ایران»، در مجموعه مقالات کنفرانس اروپایی ـ آسیایی توسعه فناوری اطلاعات و ارتباطات و همایش بین‌المللی توسعه الکترونیک و فناوری اطلاعات استان فارس، دانشگاه شیراز، صص. ۹۷-۸۸، ۹-۷ آبان.

۲٤ــ نصیری‌مفخّم، فریا (۱۳۸۲)، *طراحی و پیاده‌سازی یک سیستم چک الکترونیکی در ایران*، پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر نرم‌افزار، دانشکده فنّی و مهندسی، دانشگاه اصفهان، شهریور.

۲۵ــ نصیری مفخّم، فریا ، نعمت‌بخش، محمدعلی، براآنی دستجردی، احمد، و کیانی افشین، (۱۳۸۲)، «پایاچک، نقطهٔ عطفی برای بانکداری الکترونیکی در ایران»، در مجموعه مقالات اولین کنفرانس بین‌المللی فنّاوری اطلاعات و دانش (IKT۲۰۰۳)، دانشگاه صنعتی امیرکبیر، صص. ۱۲۷-۱۲۰، ۱۱-۹ دی.

۲٦ـ نصیری‌مفخّم، فریا، محمدعلی نعمت‌بخش و احمد براآنی دستجردی (۱۳۸۳)، «رهیافتی به سمت چک الکترونیکی با تحلیل نظام پرداخت چک در ایران»، پژوهش‌نامهٔ بازرگانی، مؤسسهٔ مطالعات و پژوهشهای بازرگانی، شماره ۳۲، پاییز، صص. ۱۰٤-۵۵.

۲۷ــ نیک‌بخش تهرانی، محمدحسن و آذر صابری، مهدی (۱۳۸۰)، آشنایی با تجارت الکترونیک و زیرساخت‌های آن (e-commerce)، انستیتو ایزایران، بهمن.

۲۸ــ وزارت کار و امور اجتماعی (۱۳۸۱)، «اصلاح قانون چک: مقالات و اظهار نظرها در مورد چک: پاسخ وزارت کار و امور اجتماعی در مورد نامهٔ چک و اشکالات موجود در ایجاد ردپای قانونی»، ۱۳۸۱/٤/۱۷، قابل دسترس در: http://www.hamafekri.org/dbase/upload/۳٤۱.pdf، رویت شده در ۱۳۸۲.