مقدمه

- پرداختهای بین المللی بانکیBIS (Bank for international settlements)
تاکید بر تفاوت بین کشورها درکاربرد چک دارد.
- درسال حدود ۲۰۰۰، حدود۴۹,۶ میلیون چک درامریکا سالیانه مورد استفاده قرار گرفت.بعدازآن فرانسه دومین کشوربوده است.
- به همین منظور جایگزینی چکهای کاغذی با چکهای مجازی برای این حجم چک وتراکنش ،بسیارمناسب است.

مزایای چکهای الکترونیک

- افزایش کارایی
- کاهش هزینه ها
- ثبات امنیت تراکنشهای مالی می شود

این چکها برای پروژههای اقتصادی بزرگ بسیار مناسب است.

عناوین

- فرایند چکهای کاغذی
- توصیف روشهایی برای مجازی کردن این رفتار
- Net cheque
- BIPS
- Echeck

فرآیند چک کاغذی

فرآیند چک کاغذی

- تحویل دفترچه چک: کاربر می‌تواند آن را مستقیما دریافت کند و یا از طریق ایمیل آن را دریافت کند.

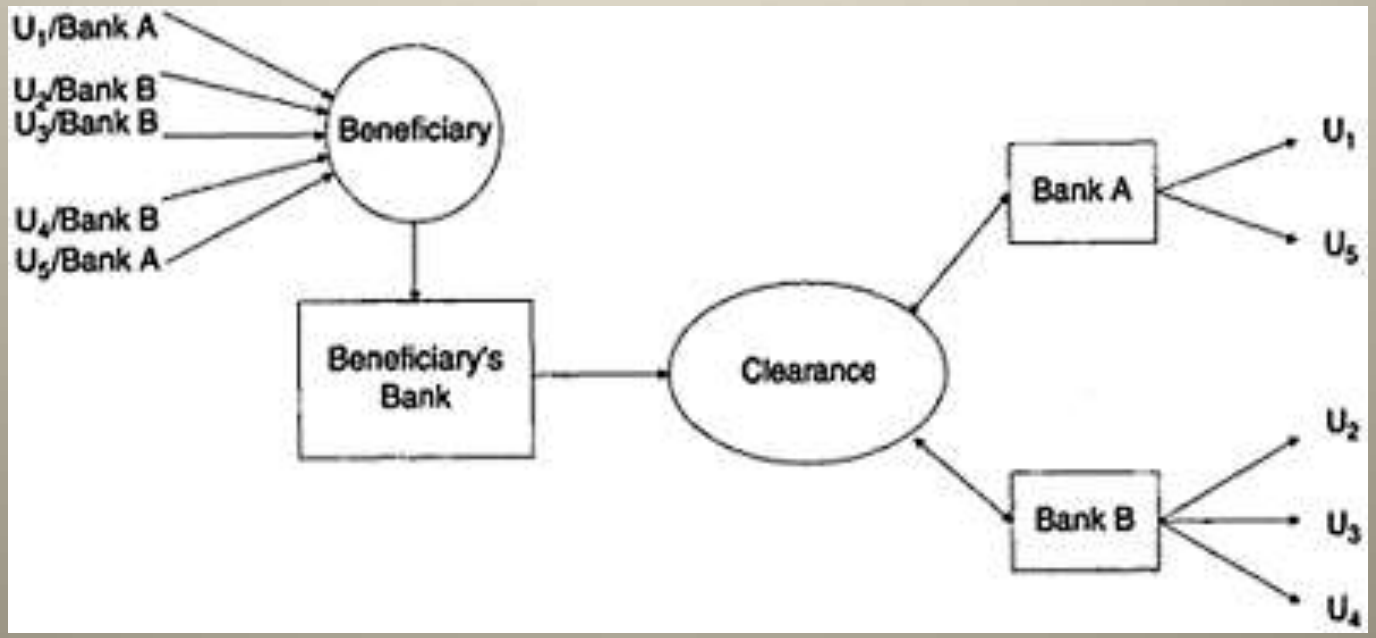
- فرآیند چک:

فرآیند انجام چکهای کاغذی در سه مرحله است:

- مرحله فرستادن
- مرحله تسویه حساب (نقل و انتقالات)
- مرحله بازگشت

تبادل فیزیکی چکها در مرحله تسویه حساب انجام می‌شود.

فرآیند چکهای کاغذی



فرآیند چکهای کاغذی

- چکها بوسیله ماشین‌ها، قطارها، هواپیما و غیره ... منتقل می‌شوند.
- نهایتا در مرحله بازگشت، بانک پرداخت کننده، امضا را تایید می‌کند و صادر کننده آن را معتبر اعلام می‌کند.
- در صورتی که چکها دارای مبالغ زیادی باشند و یا شرایط غیر عادی داشته باشند، نیاز به تاییدیه‌های اضافه تری می‌باشد.
- چکهای رد شده به صورت مجزا برگشت داده می‌شوند. این چکها خالی و بی ارزش هستند. مثلا اگر حسابی موجودی کافی نداشته باشد آن حساب بسته می‌شود یا حساب نامعتبر، یا حسابهایی که بلوکه شده‌اند یا چکهای بی محل.

فرآیند مجازی کردن چکهای کاغذی

تکنیکهای مجازی کردن چکهای کاغذی به دو دسته تقسیم می‌شوند.

۱. برای نمایش چکهای الکترونیکی، بانک ذینفع اطلاعات رابه بانک صادر کننده می‌فرستد که این اطلاعات هویت چک را مشخص می‌کند.
۲. تصویر چک، بانک ذینفع تصویر اسکن شده‌ای از چک می‌فرستد.

نمایش چکهای الکترونیکی

همان دادههای چک کاغذی را نشان می‌دهند. با حذف کاغذها بعد از ارائه به بانک، چک دریافت شده و دادههای پرداخت به صورت قالب الکترونیکی تبدیل می‌شوند و سپس به نقل و انتقالات شبکه ای و بانکی منتقل می‌شوند.

- بانکها امروزه چک کاغذی را بایگانی می‌کنند.
- هدف از این کار: جلوگیری از انتقال فیزیکی چکها و کاهش هزینه‌های نقل و انتقال بین بانکی و افزایش ضریب امنیتی است.
- آمریکا ورژن تصویری چک را ECP می‌نامد (Electronic check presentment) که در سال ۱۹۹۶ در انجمن خانه تسویه نیویورک معرفی شده بود.
- هدف از ECP، کاهش هزینه‌ها نیست بلکه جلوگیری از سوء استفاده کاربران در تاخیر زمانی بین تبادلات فیزیکی چکها و دسترسی به وجوه می‌باشد.

Point- of – sale check Approval

- سرویس Pilot که به آن Safe check در آمریکا گفته می‌شود، به وسیله موسسات پرداخت مقادیر خورد (Svpco) (Small value payment co) گسترش یافته است.
- این موسسات ECP و فرآیند کارت اعتباری را با هم ترکیب می‌کنند. که این زیر ساختی را برای انتقال وجوه الکترونیکی ایجاد می کند تا احراز هویت زمان واقعی چکها را برای ارائه شدن در نقطه‌ای از بازار فراهم کند.
- دادهها به بانک صادر کننده (بانک مشتری) منتقل می‌شود تا دسترسی به وجود و احراز و تصدیق تراکنش تایید شوند. چکهای تایید شده، لغو می‌شوند و به مشتری برگشت داده می‌شوند. مزیت این روش این است که زیر ساختی را برای تراکنش‌های اعتباری فراهم می‌کند تا خرید به وسیله چکها را تسهیل بخشد. مشکلات آن گستردگی قالبهای MICR و نیاز به، بروزرسانی دادههای پردازش و تجهیزات شبکه‌ای می‌باشد.

تصویر برداری چک

- تصویر چک عکس دیجیتالی از هر دو طرف چک به جای انتقال چک فیزیکی در شبکه‌های بانکی است. تصویر دیجیتالی را می‌توان از طریق شبکه رایانه‌ای منتقل کرده که در بانکهای مختلف ذخیره شده و به کاربر فرستاده می شود به جای چکهای فیزیکی.

- موفقیت چنین طرحی نیاز به :

۱. استفاده از الگوریتم‌های فشرده سازی تصویر دارد.

۲. علاوه بر آن تبادل امن بر روی شبکه‌های کامپیوتری را نیاز دارد.

روندروش تصویر برداری چک

- در این طرح، بانک ارائه دهنده چکی که باید به فروشنده بدهد را دریافت می کند و آن را به تصویر چک تبدیل می‌کند. سپس به کامپیوتر (Clearing) منتقل می‌کند.
- همچنین بانک ارائه دهنده مسئول آرشیو تصویر است. آن شامل فایل تصویر مراجع راهنماست که اجازه می‌دهد تا محل تصاویربرای دسترسی و بازیابی تصاویر آرشیو مشخص شود.

روندروش تصویر برداری چک

- در ۱۹۹۲، FATC (کنسرسیوم تکنولوژی خدمات مالی، On line)
(Financial services Technology consortium)که به برنامه‌های کاربردی فناوریهای جدید برای خدمات مالی وابسته است، یک پروژه در U.S،به نام PACES(Paperless Auto mated check Exchange & settlement)
(تسویه و تبادل اتوماتیک چک بدون کاغذ)، برای امکان سنجی ایجاد یک سیستم ملی برای تبادل تصاویر چک (FSTC)راآغازکرد.
- یک پروتکل بنام CIIP (Check image interchange protocol) (پروتکل مبادله تصاویر چک) انتقال فایل تصویر را توسعه داده است فرمت فایل تصویر در ANSI X9.46 (1997) مشخص شده است.

Net Cheque

Net Cheque

- *Netcheque یک سیستم آزمایشی برای چکهای مجازی،*

از موسسه علمی اطلاعات (ISI) از دانشگاه کالیفرنیای جنوبی (USC) است.

(ISI) : Information Science Institute

- در اصل، آن برای مدیریت توزیع شده دسترسی به منابع محاسبات در مرکز محاسبات دانشگاه هماهنگ شده بود. این منابع می‌تواند، به عنوان مثال، مقدار بلوک حافظه اختصاص داده شده، تعداد چرخه‌های فرآیند، یا تعداد صفحات چاپ شده و غیره داشته باشد.

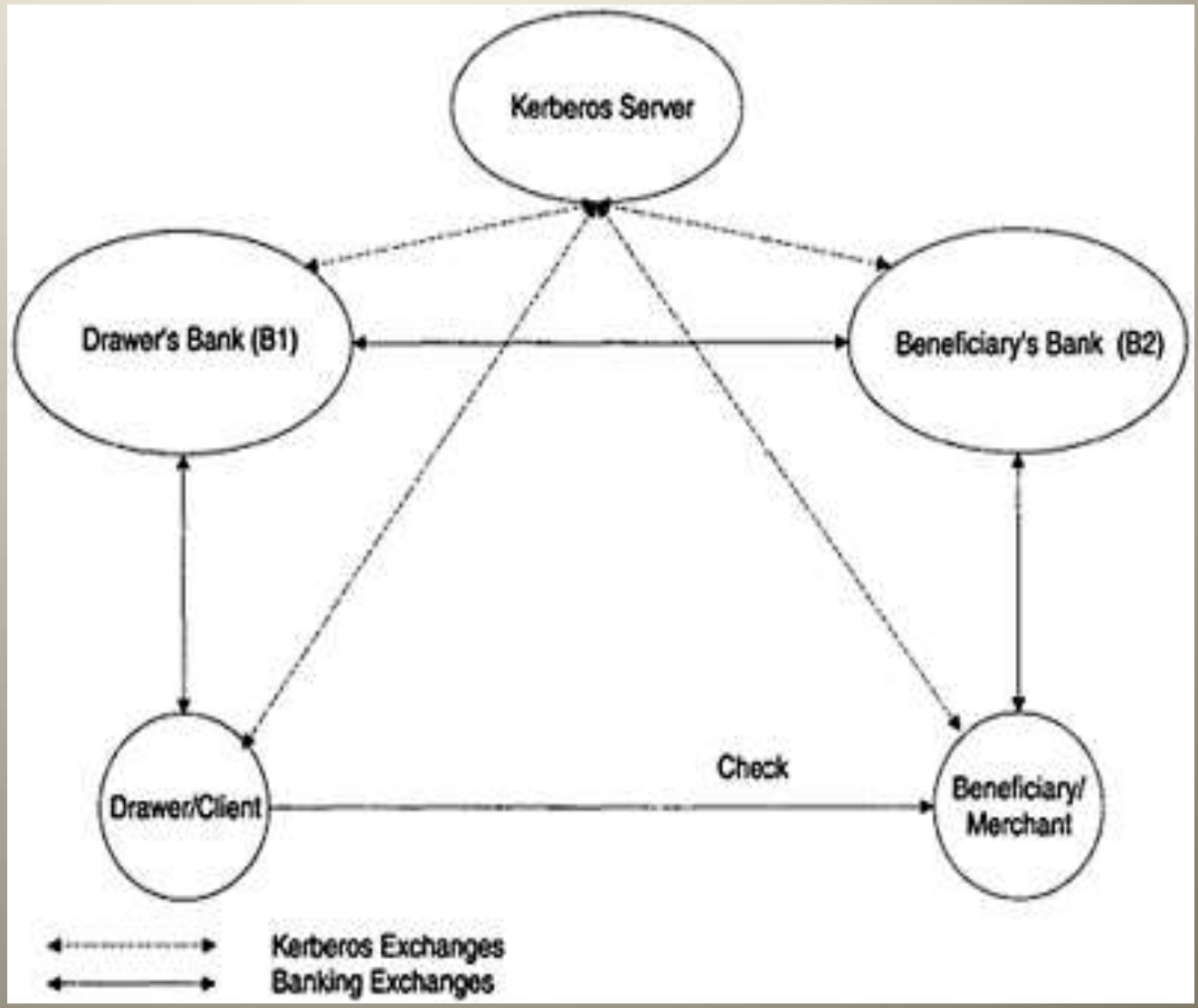
Net Cheque

از Kerberos برای احراز هویت وتولید وتوزیع کلید جلسه استفاده می شود.

سه کلید جلسه مورد نیاز:

- کلید K_{CB1} کلیدی بین مشتری و بانک آن (B_1)
- کلید K_{MB2} کلیدی بین تاجر و بانک خود (B_2)
- کلید K_{BB} کلید جلسه بین دو بانک

به طورکلی سرور کربروز از دوبانک مجزاست



Net Cheque

گواهینامه مشتری با توجه به بانک مشتری یک بلیط نشست است که منابع سرورکربروزویک اعتبار دهنده اتوماتیک مشتری به نام (authenticator Authc)به آن ساختار می دهدوبا کمک کلید نشست رمز نگاری می کند.

Net Cheque

ثبت نام

کاربران در بانکهای خود با افتتاح حساب ثبت نام می‌کنند و سپس چک مجازی می‌گیرند. هرحساب با شناسه سرورهای بانک تعریف شده است.

- نام کاربرازلیست مجوزهای دسترسی، و مجموعه مانده حساب برای هر یک از پولهای رایج (پولهای منتشر شده) که می‌تواند مورد استفاده قرار گیرد تشکیل شده است.

چکهای مجازیNet chequeشامل موارد زیراست:

- مقدار
- نوع پول
- تاریخ چک
- شماره حساب مشتری
- نام فروشنده
- امضای دیجیتال دارنده حساب
- تایید فروشنده که ازبانکش استفاده می‌کند.

بانک مشتری دو فیلد آخر را تایید می‌کند در حالی که فیلدهای باقیمانده به صورت آشکار فرستاده شده است.

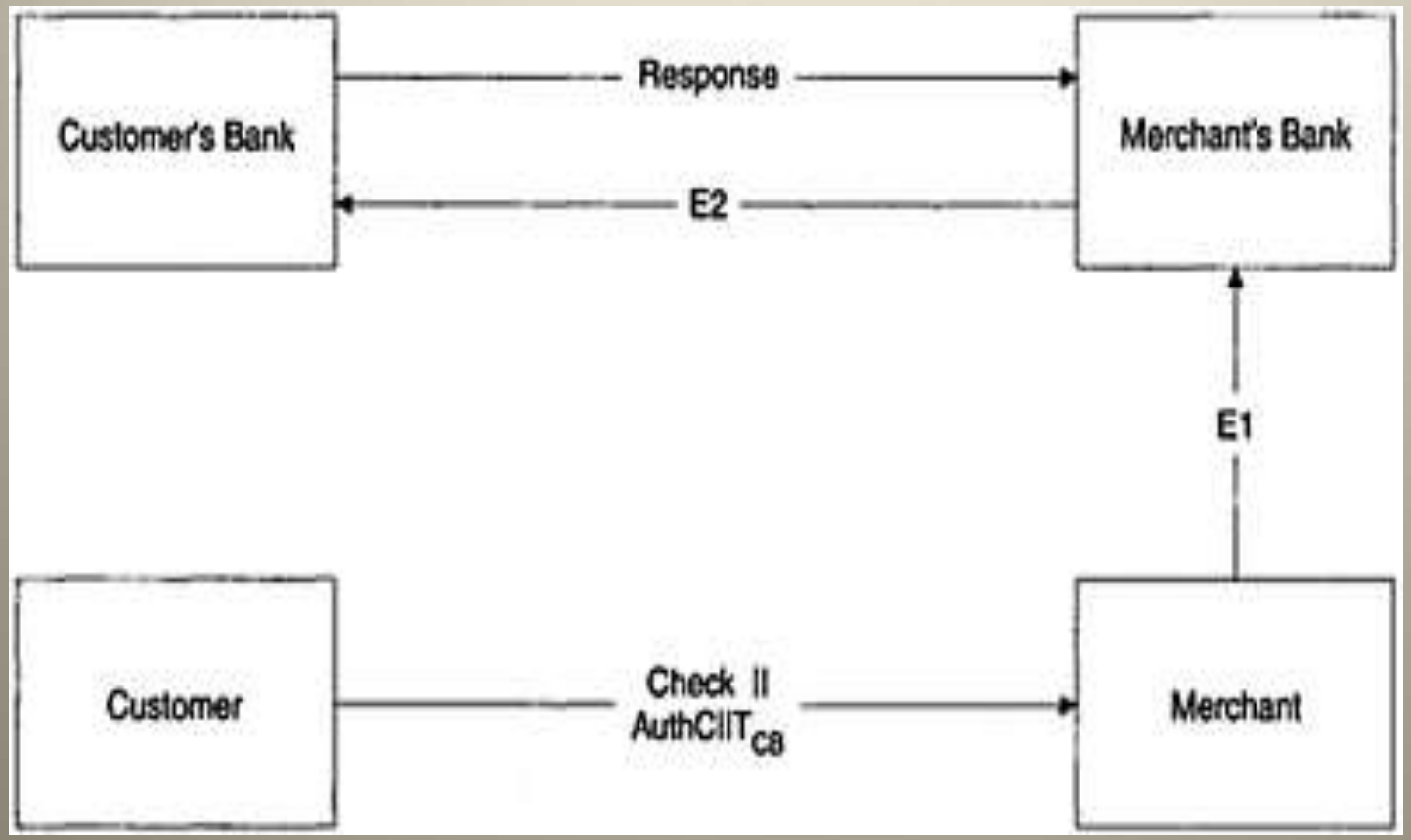
فیلدهای آشکارتهدیدات Net Cheque است.

Net Cheque

پرداخت و توافق مالی:

- طراحی یک چک، دادن به فروشنده یعنی حق انتقال سرمایه از حساب مشتری است.
- مشتریان از یک بلیط Kerberos, T_{CB} برای احراز هویتشان به بانکشان (B_1) استفاده می‌کنند.
- به طورمشابه تاجر به بلیط T_{MB} نیاز دارد برای احراز هویت خود به بانکش (B_2)
- در نهایت بلیط T_{BB} اجازه می‌دهد بانک B_2 به بانک B_1خودش را احراز کند (احراز هویت B_2 به B_1)

تبادلات در هنگام پرداخت با استفاده از چکهای مجازی با توجه به Net cheque



Net Cheque

بلیط نشست T_{CB} شامل:

اطلاعات در این میان، شناسایی S سرور Kerberos،نام مشتری C، مختصات بانکی B_1 و کلید نشست K_{CB}. محتوای بلیط جز شناسایی سرور، با کلید K_{SB1} رمزنگاری میشود بین سرور Kerberos و بانک مشتری (B_1)مبادله می شود.

$$T_{CB} = \{ S, K_{SB1} (C, B_1, K_{CB})\}$$

به طور مشابه، بلیط T_{MB} حاوی اطلاعات مشابه برای تاجر است

$$T_{MB} = \{ S, K_{SB2} (M, B_2, K_{MB})\}$$

Net Cheque

در نهایت بلیط T_{BB} مشخص می شود با:

$$T_{BB}= \{S, K_{SB1}(B_2, B_1, K_{BB})\}$$

- احراز هویت کننده ساختار مشتری، Authc، حاوی احراز هویت مشتری C، شماره حساب مشتری Noc و خلاصه چک است. و همه اطلاعات با کلید نشست K_{CB} رمزنگاری شده است:

$$\text{Auth C} = k_{CB} \{H (\text{check})\}$$

Net Cheque

- احراز کننده آن رارمزنگاری می‌کند و با کلید نشست(پیوست شده) به چک، پیام به تاجر فرستاده می‌شود.

Check || Auth C || T_{CB}

- در شیوه ای مشابه، تاجر یک کانال ارتباطی امن با بانک خود ایجاد می‌کند و از بلیط T_{MB} برای نشست استفاده می‌کند.
- برای تایید چک (پشت نویسی و امضا)،ساختارهای یک احراز کننده Auth M:

Auth M= K_{MB} {H (Check)}

Net Cheque

- فروشنده تایید احراز کننده‌اش را به پیام دریافت شده توسط مشتری الحاق می‌کند. پیام E_1 که به بانک فروشنده فرستاده شده به فرم زیر می باشد.

$$\mathbf{E_1 = Check \,||\, Auth\ C \,||\, T_{CB} \,||\, Auth\ M \,||\, T_{MB}}$$

- بانک فروشنده، چک را با ساخت احراز کننده Auth Bرا تایید می کند.

$$Auth\ B = K_{BB}\{H(Check)\}$$

- بلیط نشست T_{BB} به پیام E_2 پیوسته می‌شود و به بانک مشتری فرستاده می‌شود به شرح زیر:

$$E_2 = Check \,||\, Auth\ C \,||\, T_{CB} \,||\, Auth\ B \,||\, T_{BB}$$

Net Cheque

- بانک مشتری تمام اطلاعات موجود در بلیط و احراز کننده اش را تایید می‌کند ،تایید این که بانک B_2 و مشتری معتبرند وسپس با کلیدهای متناظر K_{CB} یا K_{BB}احراز کننده ،رمزگشایی را انجام می دهد.

سیستم پرداخت اینترنتی بانک Bank internet Payment System (BIPS)

- BIPS و echeck در میان چندین پروژه برای چکهای مجازی هستند که FSTC ترویج یافته هستند.
- مشابه الکترونیکی از دسته چک هستند که در برابر مداخله کارت ریز پرداخت مورد استفاده خواهند بود.
- هدف BIPS از طراحی سیستم پرداخت راه دور با استفاده از اینترنت این است که از ارتباطات پشتیبانی کند.
- این برنامه کاربران زیادی از چک، مانند حرفه‌ایها (افراد حرفه‌ای)، شرکتها، و بانکها آنها را هدف قرار می‌دهد. به این ترتیب، سیستم پرداخت حقوق و دستمزد، پرداخت برای خدمات و بازپرداختها، از یک شرکت یا سازمان دولتی به افراد و یا شرکتهای دیگر را پوشش می‌دهد. تبادل می‌تواند تعاملی از طریق وب و یا از طریق پست الکترونیکی باشد.

BIPS

- یکی از جاه طلبیهای BIPS این است که به طور کامل جایگزین مکانیزمهای ارتباطات Inter banking در سطح جهانی شود، که آن را در رقابت با شبکه های موجود مانند SWIFT قرار می‌دهد.
- BIPS دو رقیب دیگر دارد: اولی OFX،دومی Check free

OFX: Open Finance Exchange

- OFX، با هدف ارائه خدمات بانکی شخصی، مانند Home bankingدر حال کار با SGML است.

SGML:(Standard Generalized Markup Language)


echeck

Echeck

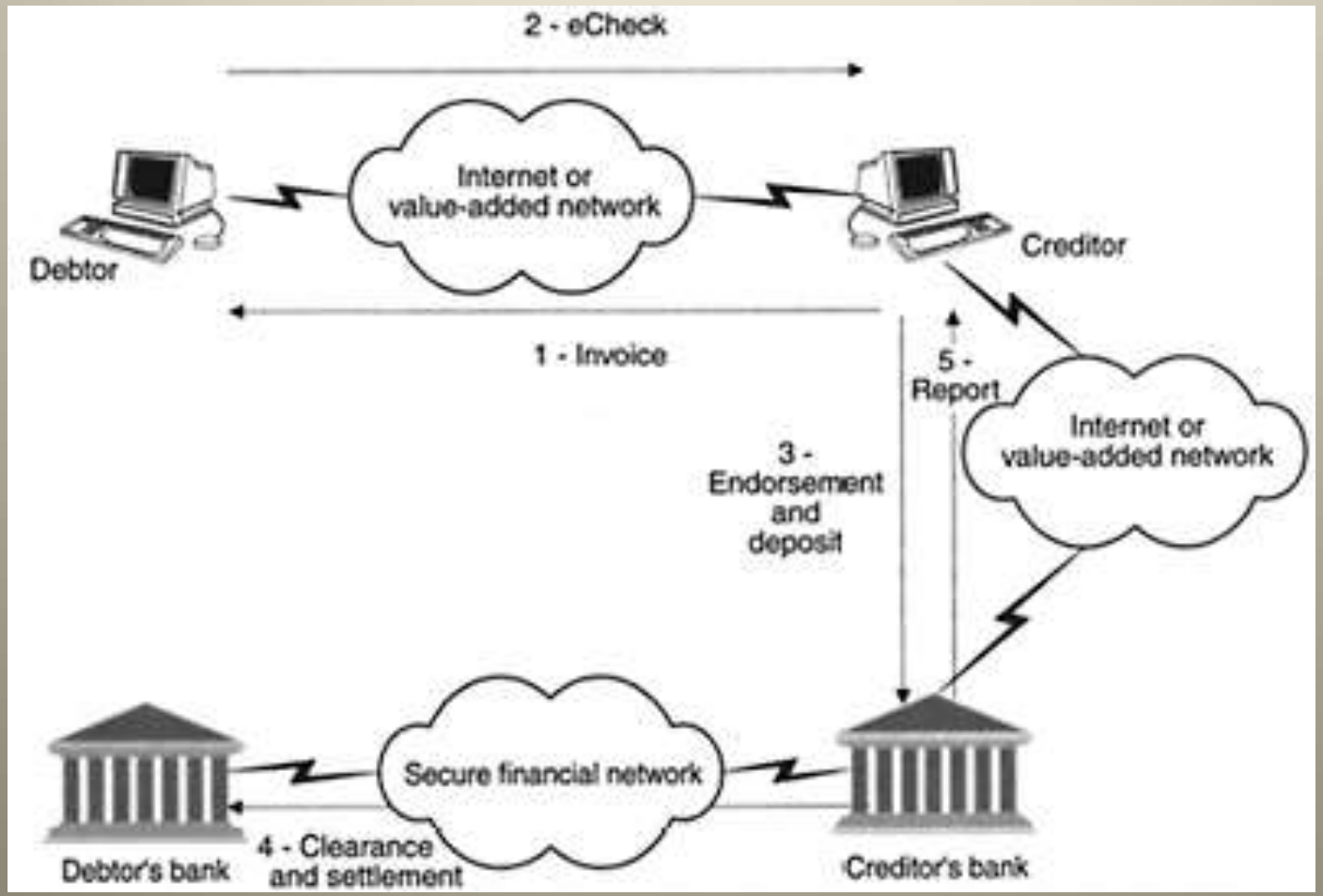
- e check یک چک مجازی است که با حمایت FSTC و وزارت خزانه داری ایالات متحده است. (Jaffe و Landry ، در 1997).
- در حال حاضر، آن تنها مکانیزم پرداخت الکترونیکی است که توسط وزارت خزانه داری ایالات متحده به رسمیت شناخته شده است وبرای هدایت یک آزمایش در وزارت دفاع برای پرداختهای بالا 100,000$در آمریکا استفاده شده بود.
- مجوز تکنولوژی e check به Clareon داده شد Clareon آن را در طرح پرداخت الکترونیکی امن pay mode خودش گنجاند.

پرداخت وتوافقات Echeck

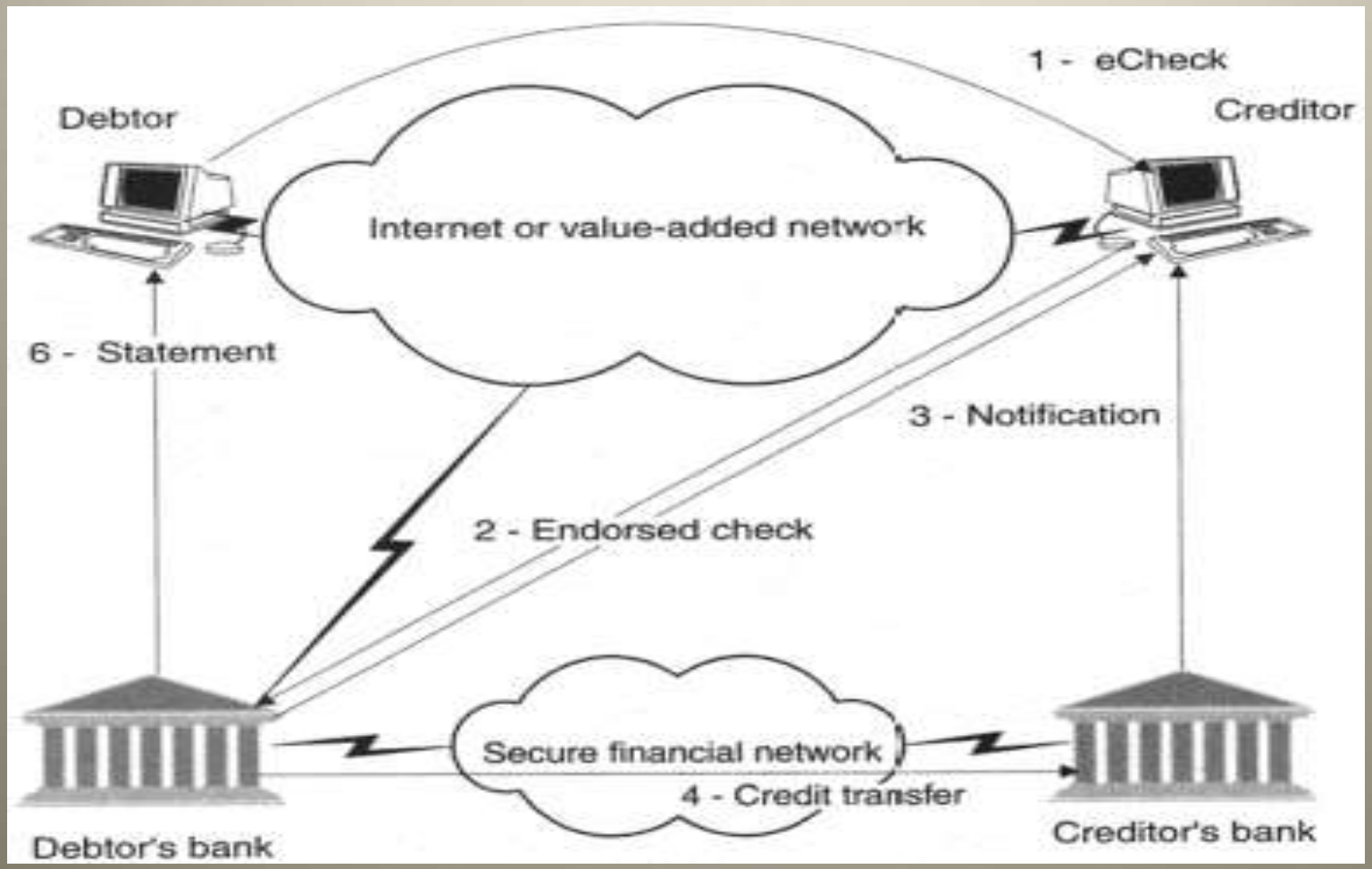
هدف این ابزار جدید اجازه دادن به یک بدهکار، چه یک موسسه یا یک فرد برای انتقال یک وجه با استفاده از پیامهای استاندارد شده ای که به وسیله e-mail فرستاده می‌شود.

گواهینامه و توافقات بین بانکی چکهای مجازی از ANSI X 9.46 (1997) و X 9.37 (1994) استفاده کرده است.

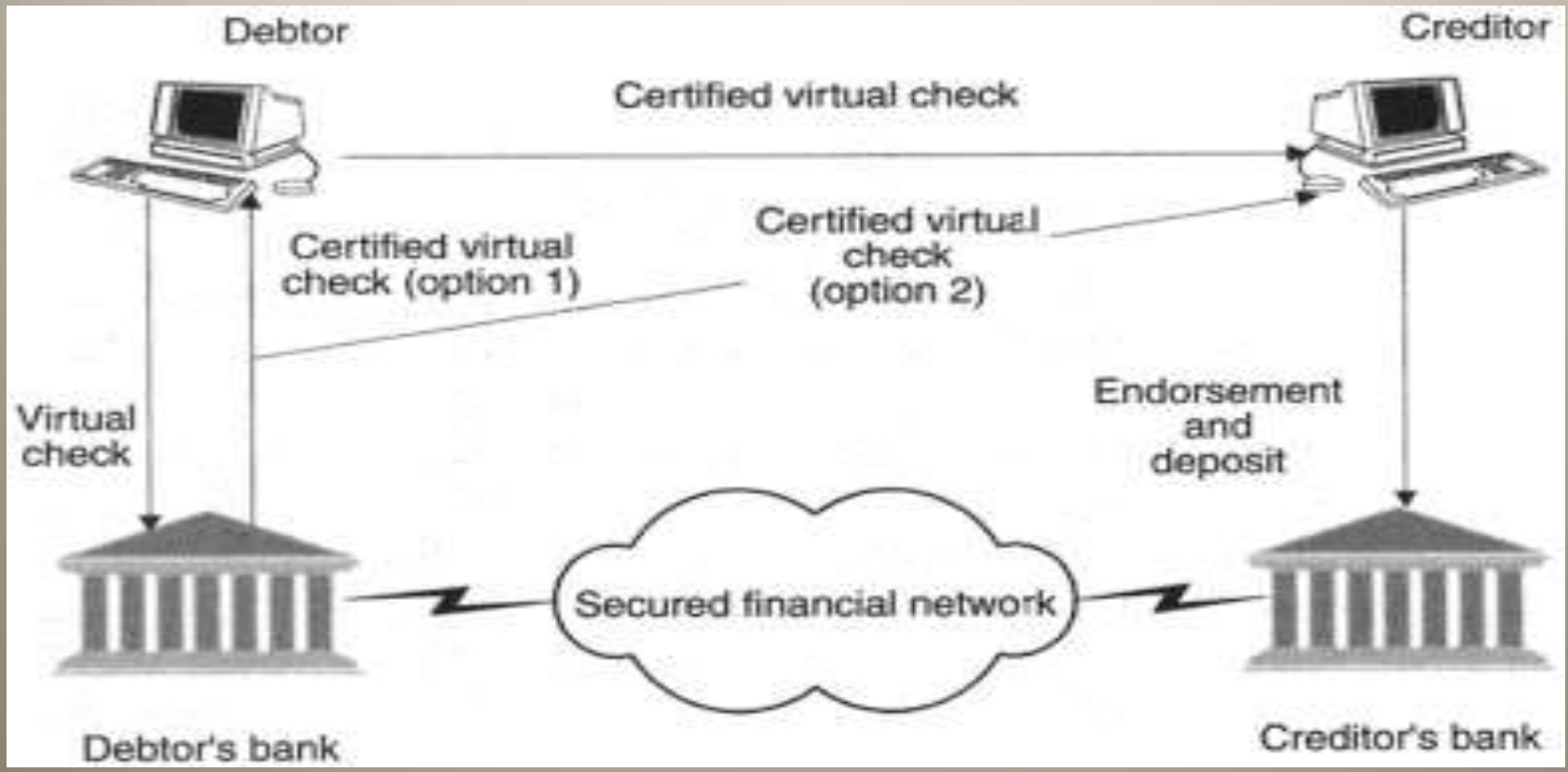
Deposit and Clear



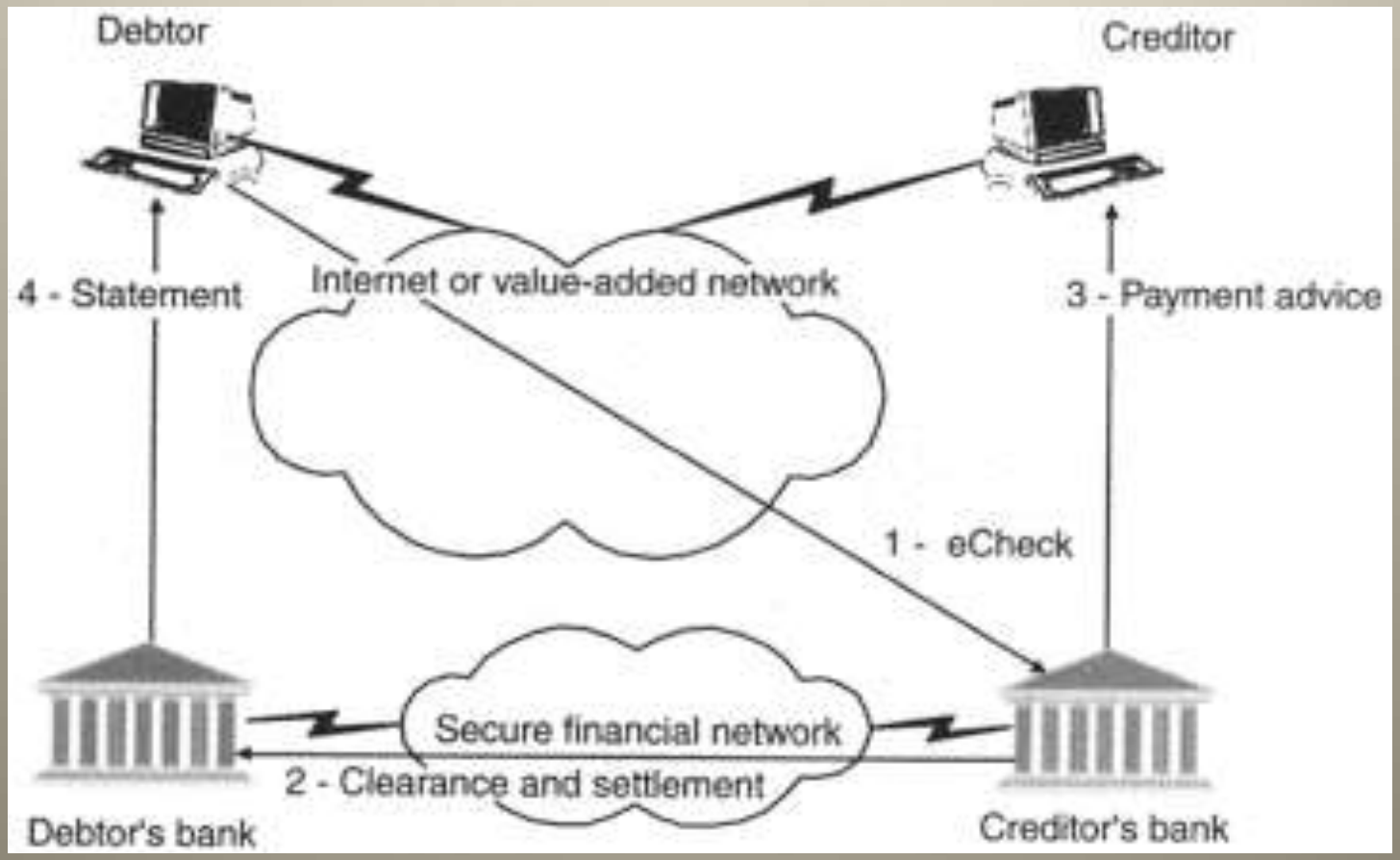
Cash and Trancfer



Exchanges for certified virtual checks with e Check



lockbox


Debtor
Creditor
4 - Statement
Internet or value-added network
3 - Payment advice
1 - eCheck
Secure financial network
2 - Clearance and settlement
Debtor's bank
Creditor's bank

نمایش چک‌های الکترونیک

- نمایش e check با استفاده از زبان نشانه گذاری (FSML) (FSTC, 1998a) است.
- این زبان در چهارچوب SDML است (Signed Document Markup language) (امضا سند زبان نشانه گذاری)، که مشخص می‌کند چطور اسناد دیجیتالی امضا شود.

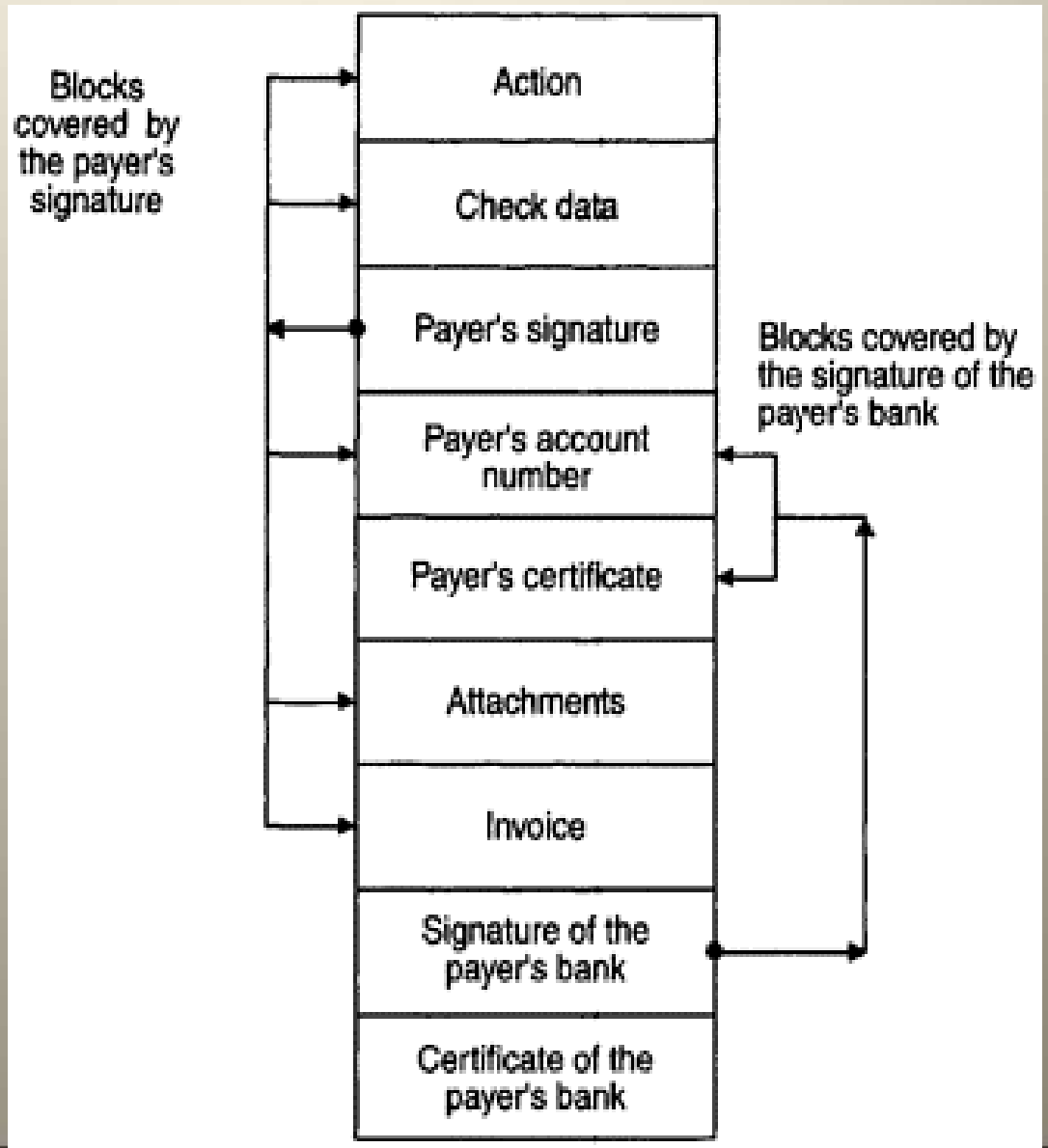
- طراحان FSML هدفشان در برنامه‌ها کاربردی مالی کارتهای ریزپردازنده‌ای بود و نتوانستند مقیاس منطقی برای آن بدست آورند که پهنای باند آزاد و حافظه فراوان می‌خواهد.
- این مایه تاسف است که دو پروژه FSTC یعنی e check و BIPS از زبانهای ناسازگاری استفاده می‌کنند.

- FSML توصیف چک با استفاده از دنباله‌ای از بلوکها برای نشان دادن اطلاعات مربوطه به چک است.این بلوک‌ها می‌تواند به صورت تو در تو باشد و با کمک الگوریتم‌های رمزنگاری کلید عمومی و الگوریتم hash برای امضا استفاده شود و رمزنگاری می‌شوند. FSML نشاندهنده کاراکترهای الفبایی هستند .
- دو مقوله در بلوک‌های یک e check وجود دارد.اولین شامل عملیات

داده‌های چک، شماره حساب بدهکار، تمام اسناد ضمیمه شده وصورت حساب است. که این به وسیله کلید خصوصی فرستنده امضا می شود.

- دسته دوم شامل شماره حساب و گواهی بدهکار است که آن با کلید خصوصی بانک امضا شده است

نمایش چک‌های مجازی در e check



توضیحات

- تایید e check به معنای اضافه کردن بلوکهای تایید است با هویت امضا کننده، مختصات بانکی‌اش، گواهی نامه‌اش، گواهی بانکی‌اش مشخص می شود.
- دو الگوریتم برای محاسبه امضا استفاده می‌شود. این الگوریتم‌ها MD_5 با RSA و SHA-1 با الگوریتم DSA هستند.

Representation of an endorsed virtual check in e Check

مقایسه‌ای چک‌های مجازی با کارتهای بانکی

ویژگیها اصلی که چکهای مجازی را از پرداخت‌های از راه دور با کارتهای بانکی متمایز می کند به شرح زیر عبارتند از:

۱. SSL/TLS و SET برای معاملات تعاملی روی وب هستند، در حالی که چک‌های مجازی یا بر روی وب و یا از طریق پست الکترونیکی استفاده می‌شود.

۲. SSL/TLS وSET ازاحرازهویت real – time استفاده می‌کنند و تایید آنلاین گواهی را می‌دهند.درمقابل،احرازهویت درمورد چک‌های مجازی لازم نیستreal – time باشد که محدودیتیههی تحمیل شده بر روی سیستم را کاهش می‌دهد.

۳. در SET، داده‌های تراکنشها رمزنگاری می‌شود و اطلاعات حساب کاربر از سرورهای تجاری پنهان می‌شود (اما نه از دروازه‌های پرداخت)

مقایسه‌ای چک‌های مجازی با کارتهای بانکی

۴- در SET، دروازه پرداخت نقش یک امانت دارد طرف سوم،را بازی می‌کند (داور و قاضی Small claims) بدون اینکه جزئیات معامله را بداند. بنابراین، آن توافقات بین خریدار و فروشنده را با استفاده از روشهای خلاصه شده تایید می‌کند. هیچ شخص ثالث مورد اعتمادی در مورد چک‌های مجازی وجود ندارد.

تفاوت پرداخت الکترونیکی توسط چک‌های مجازی و کارتهای بانکی از طریق SET

SET	چکهای مجازی	مشخصات
کارتهای بانکی (Credit and debit)	چک‌های مبتنی بر کاغذ	مدل پرداخت منتشرشده
Web	e-mail – web	تعامل با کاربر
On line	Off line	احراز هویت
پیش مجوز (در زمان) تعهد پرداخت	به طور پیوسته با دستورالعمل پرداخت ارسال	مجوز پرداخت کننده
اجباری	در دسترس نمی‌باشد	شخص سوم مورد اعتماد
از فروشنده پنهان شده	در دسترس فروشنده	اطلاعات مربوط به حساب پرداخت