جلسه ۱۵

* پروتکل e-cash : پروتکل پرداخت پول الکترونیکی

دلایل متعددی وجود دارد که ممکن است کاربر مصرف کننده به علت استفاده از پول‌های تحت web بردد. برخی از این دلایل در زیر آورده شده است:

① امنیت بیشتر مبادلات نسبت به کارت های اعتباری

② توانایی خریدهای اینترنتی با حجم پایین

③ گمنامی مبادلات و عدم امکان ایجاد ارتباط بین پول و شخص خریدار

④ هزینه کم مبادلات

* در پروتکل e-cash ، گمنامی خریدار مهمترین عامل در طراحی پروتکل است.

روز بزرگداشت محمدبن زکریای رازی ، روز داروسازی ، روز کشتی

۶ پنجشنبه شهریور ۱۳۹۹ — محرم ۱۴۴۲ — 27 Aug 2020

* موجودیت های دخیل در پروتکل e-Cash :

- بانک ها (پول صادر کننده) : بانک هایی که سکه ها را ضرب می کنند، سکه های موجود را تایید می کنند و پول واقعی را برای eCash مبادله می کنند
- خریدارانی که نزد بانک حساب دارند و می توانند سکه های e-Cash (پول های eCash) را از حساب هایشان برداشت کنند یا به آن واریز کنند.
- بازرگانانی که می توانند سکه های e-Cash را برای پرداخت هزینه اطلاعات یا محصولات فیزیکی دریافت می کنند. همچنین بازرگانان این امکان را خواهند داشت که سرویس pay-out را برای شرایطی که می خواهند به کسی مشتری سکه های e-Cash را پرداخت کنند اجرا کنند.

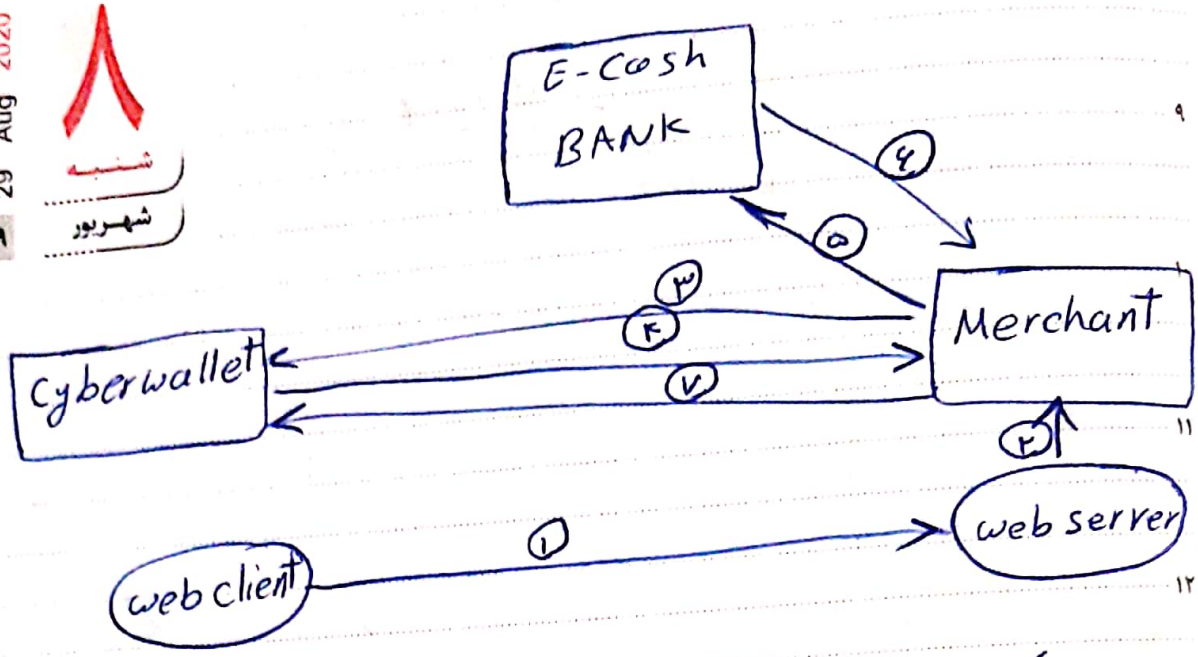
۷ جمعه شهریور ۱۳۹۹ — محرم ۱۴۴۲ — 28 Aug 2020

- صنای پروتکل e-Cash امضای کور می باشد.

امضای کور: نوعی از امضا است که در آن امضا کننده نمی تواند ببیند چه چیزی را امضا کرده است.

۸ محرم ۱۴۴۲ | ۲۹ Aug 2020 | ۸ | شنبه | شهریور ۱۳۹۹

* مراحل انجام معامله در پرداخت e-cash



کاربری پرداخت e-cash & * خریدار با درخواست مشتری صورت می‌گیرد.

① درخواست خرید مشتری (از طریق مرورگر وب شروع می‌شود)

② درخواست از بازرگان ← پس از درخواست مشتری بازرگان درخواست را بررسی می‌کند.

۹ محرم ۱۴۴۲ | ۳۰ Aug 2020 | ۹ | یکشنبه | شهریور ۱۳۹۹

③ درخواست پول از مشتری ← بازرگان درخواستی حاوی مبلغ پرداختی برای مشتری ارسال می‌کند

④ ارسال پول ← مشتری درخواست را دریافت و تأیید می‌کند

⑤ درخواست بررسی صحت ← مشتری با شبکه مالی تماس برقرار می‌شود و بررسی می‌کند تا پول را پرداخت کند

⑥ ارسال نتیجه ← نتیجه بررسی شرایط مالی مشتری به بازرگان و پرداخت پول

⑦ ارسال رسید برای مشتری

در صورت پرداخت رسید ارسال می‌شود.

۸ تاسوعای حسینی (تعطیل)، روز مبارزه با تروریسم (انفجار دفتر نخست وزیری به دست منافقان و شهادت مظلومانه شهیدان رجایی و باهنر، ۱۳۶۰ هـ‌ش) ۹ عاشورای حسینی (تعطیل)

۱۰ دوشنبه 31 Aug 2020 محرم ۱۴۴۲ شهریور ۱۳۹۹

* معرفی پروتکل e-cash: چگونه مشتری پول را از حساب خود برداشت می‌کند؟ (رمزنگاری با توابع یک‌طرفه انجام می‌شود)

① بانک ابتدا دو عدد اول بزرگ p و q را انتخاب کرده و حاصلضرب آنها ($n = p*q$) را به عنوان کلید عمومی (کلید عمومی) در نظر می‌گیرد

② مشتری آنلاین برای برداشت پول از Cyberwallet خود یک عدد سریال x و یک ضریب کور کننده r را می‌سازد. x یک عدد ۱۰۰ رقمی است.

③ مشتری آنلاین x را از تابع یک طرفه f رد کرده f(x) را می‌سازد. سپس می‌عدد زیر را محاسبه می‌کند (خاصیت این تابع هم‌ریخت بودنش است)

$$B = ((f(x) * r) \bmod n)$$

(ضریب سریال)

فرض کنید که توان 5 در این جا نشان دهنده 2 دلار است (توان‌های مختلف نشانگر مقادیر مختلف پول می‌باشند. به طور مثال 1 دلار با عدد 3 و 2 دلار با عدد 5 و ... مشخص می‌شود) سپس آنلاین B را به بانک می‌فرستد. مشخص کننده مبلغ برداشتی مشتری از حساب است.

④ بانک رشته پیغام B را گرفته عبارتی D را به گونه‌ای محاسبه می‌کند که

$$(D^5) \bmod n = B$$

برای این منظور ابتدا inv1 به گونه‌ای محاسبه می‌شود که

روز تجلیل از اسرا و مفقودان

۱۲۱

$(5 * INV1) \bmod (p-1)(q-1) = 1$

سپس $ID = (B \hat{} inv1) \bmod n$

فرمول بالا می‌تواند به صورت زیر نوشته شود.

$D = ((f(x) \hat{} (1,5)) * r \bmod n$

بنابراین گرفتن ریشه پنجم B همانند این است که بانک پول را امضاء کرده است. این امضاء می‌تواند توسط دریافت کننده پول کنترل شود

نکته دیگر این که بانک x و $f(x)$ را ندارد بنابراین بانک 2 دلار از حساب آلیس برداشته و D را برای آلیس می‌فرستد

آلیس با تقسیم D بر r، C را به دست می‌آورد یا به عبارتی C را چنان پیدا می‌کند که:

$D = (C * r) \bmod n$

برای این منظور Inv2 نگونه‌ای می‌سنجد می‌شود که

$(r * Inv2) \bmod n = 1$

سپس:

$C = (D * Inv2) \bmod n$

$C = (f(x) \hat{} (1,5)) \bmod n$

مبلغ پول

اکنون آلیس x و C را ارسال می‌کند (رمز شده با امضای کور)

پول الکترونیکی را امضا می‌دهند. بصورت عملی داده

یک پول الکترونیکی شامل نام بانک، مقدار پول، x و C می‌باشد

* مشتری چگونه پول را خرج می‌کند؟

① برای پرداخت 2 دلار به باب، به او (x, C) می‌دهد

② باب برای اینکه مطمئن شود که پول توسط بانک صادر شده است C را به توان d می‌رساند و آن را با $f(x)$ مقایسه می‌کند. حال باب (فروشنده) برای اینکه مطمئن شود که این پول قبلاً خرج نشده است (x, C) را به بانک می‌فرستد

③ بانک x را چک می‌کند آیا قبلاً استفاده شده است یا خیر؟ در صورت استفاده نشدن به باب اطلاع داده و 2 دلار به حساب وی واریز می‌کند. در واقع بانک لیست کلیه x ها را نگه می‌دارد