FAPSWPP : یک پروتکل خرید امن کالای الکترونیکی مبتنی بر APSWPP

نگارندگان:
سمانه لایقیان جوان
عباس قائمی بافقی

مقدمه

پرداخت الکترونیکي : ارسال پرداخت ها برروي يك شبكه عمومي براي به دست آوردن كالا (الكترونيكي و يا فيزيكي) و خدمات.

نیاز به امنیت بالا به دلیل ارسال اطلاعات حساس و محرمانه از طریق شبکه

ویژگیهای امنیتی مورد نیاز سیستمهای پرداخت

- تایید هویت
- عدم انکار
- محرمانگی داده ها
- در دسترس بودن

- حفظ حریم خصوصی
- تمامیت داده ها
- گمنامی
- تایید دسترسی

مبادله منصفانه

- در تراکنشهای خرید کالاهای الکترونیکی این نیاز امنیتی نیز به چشم می خورد.
- در معاملات الکترونیکی افراد غالباً مکان فیزیکی قابل شناسایی و مشخصی ندارند. هر یک از طرفین می تواند بدون انجام کامل تعهدات خود ناپدید شود.
- پروتکلهای خرید الکترونیک باید به گونه ای طراحی شوند که امکان این گونه از تخلفات برای هیچ یک از طرفین وجود نداشته باشد. به چنین معامله ای، مبادله منصفانه می گویند که به دو دسته تقسیم می شود:
  - پروتکلهای تبادل تدریجی
  - پروتکلهای تبادل خوشبینانه

پروتکل پیشنهادی

- توسعه SWPP جهت تامین ویژگیهای گمنامی و حریم خصوصی مشتری (APSWPP)
- توسعه APSWPP جهت تامین ویژگی تبادل منصفانه (FAPSWPP):
  - اطمینان مشتری از دریافت کالا در قبال پرداخت وجه
  - اطمینان فروشنده از دریافت وجه در قبال تحویل کالا
  - اطمینان فروشنده از دریافت رسید امضا شده در قبال تحویل کالا
- استفاده از یک شخص ثالث مورد اعتماد جهت تامین ویژگی تبادل منصفانه
- استفاده از روش تبادل خوشبینانه (رجوع به شخص ثالث تنها در صورت بروز اختلاف)

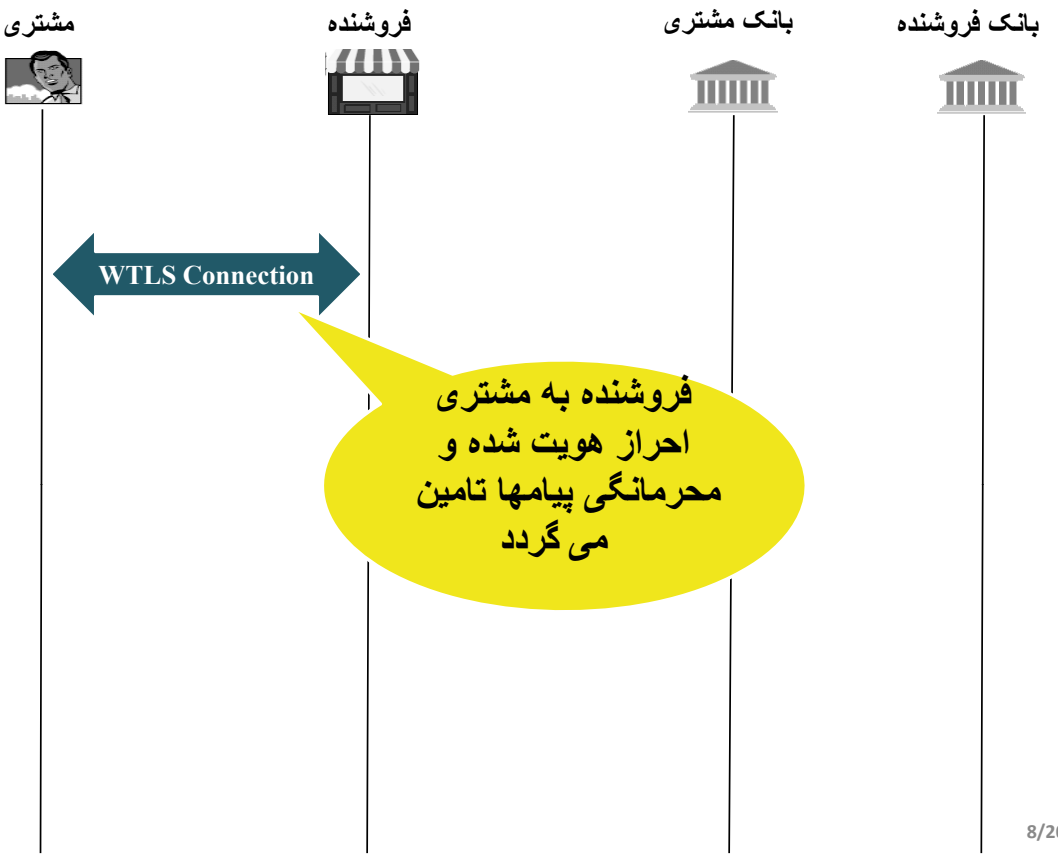
مراحل پیش از انجام تراکنش

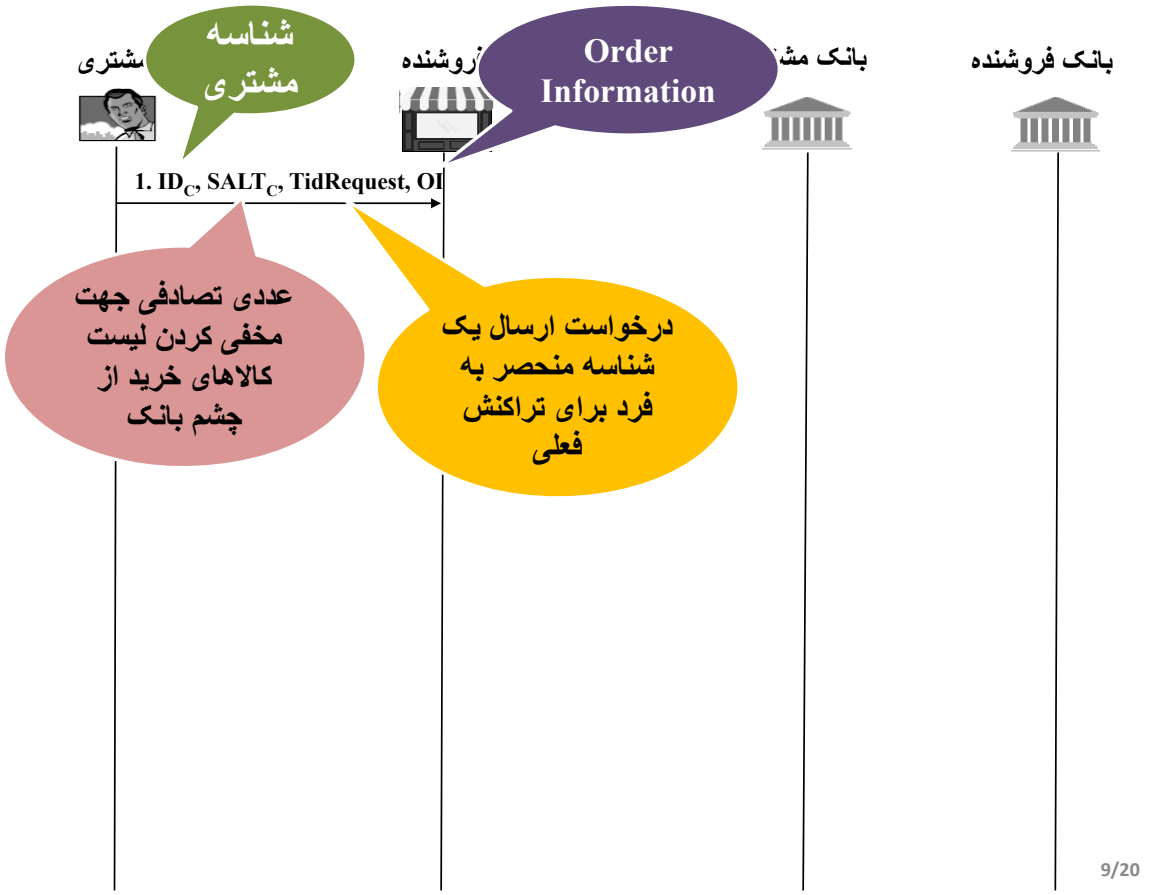
- گواهینامه دیجیتال با نام مستعار برای مشتری
- ایجاد یک حساب بانکی گمنام برای مشتری و پیوند دادن کلید عمومی مشتری به این حساب
- ارسال رمز مخفی K_A و شماره حساب acc_A به صورت امن برای مشتری

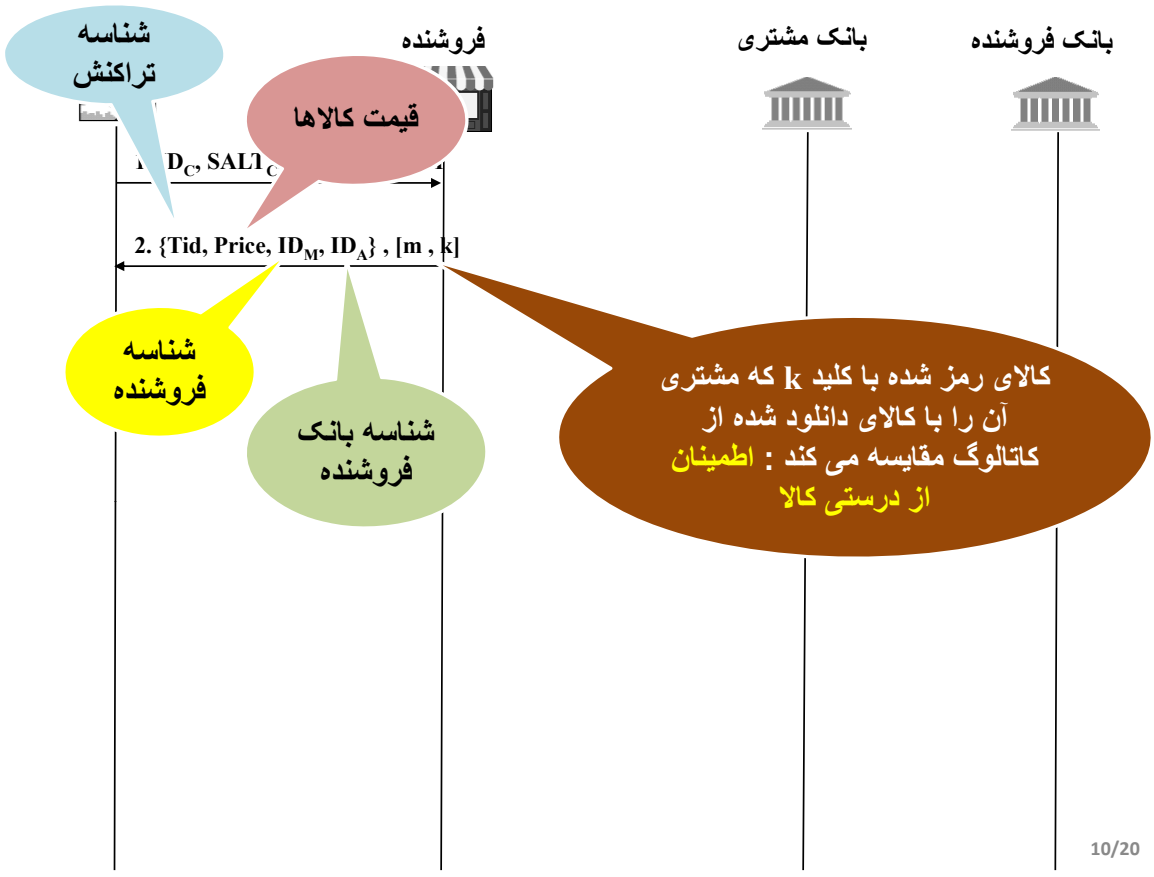
مراحل پیش از انجام تراکنش

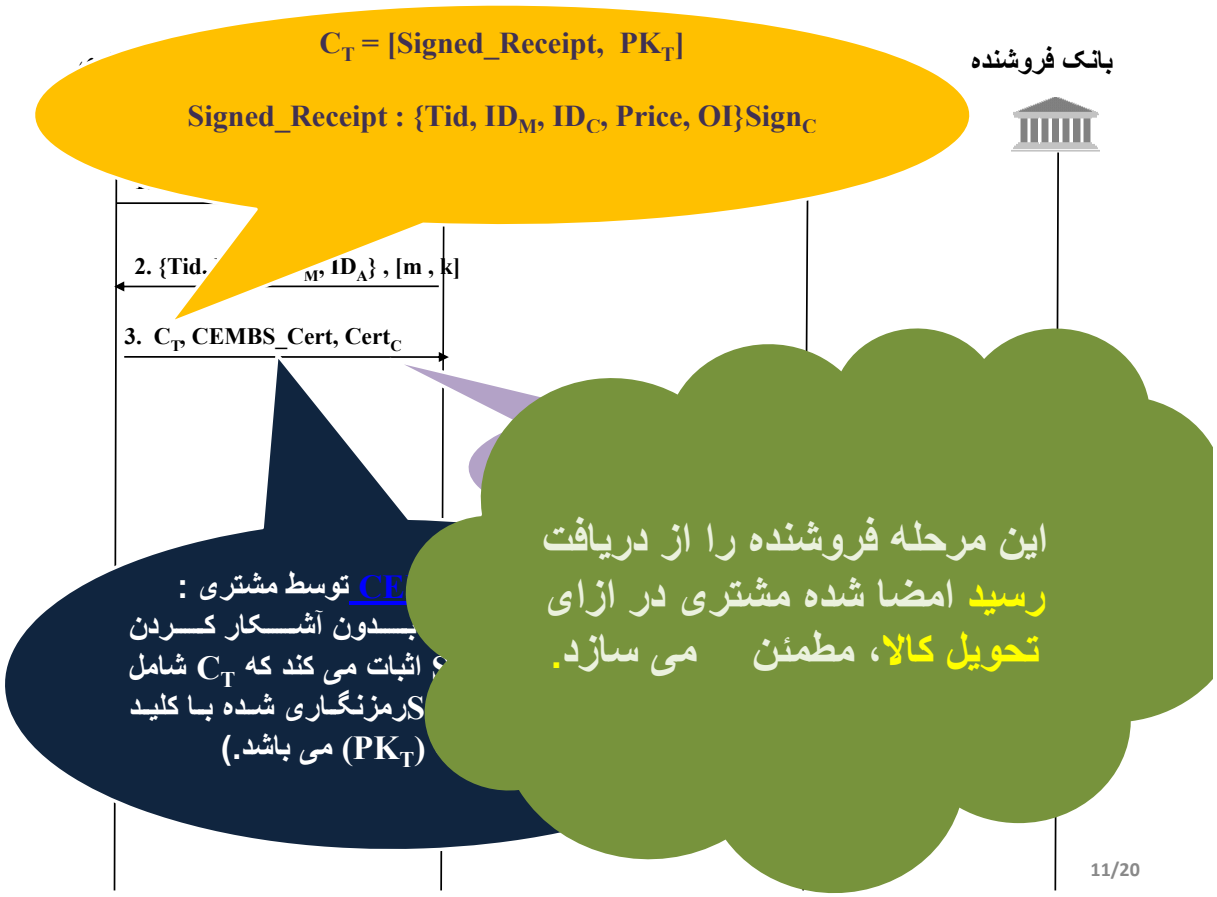
- ثبت نام فروشنده در یک شخص ثالث مورد اعتماد
- ارائه کالاهای فروشنده و توصیف آنها به شخص ثالث جهت تبلیغ کالاها در کاتالوگ
- رمزنگاری هر کالا توسط یک کلید رمزنگاری k پیش از قراردادن کالا در کاتالوگ و ارائه کلید k به فروشنده
- دانلود کالای رمز شده m ([m, k]) از کاتالوگ شخص ثالث جهت خرید کالا

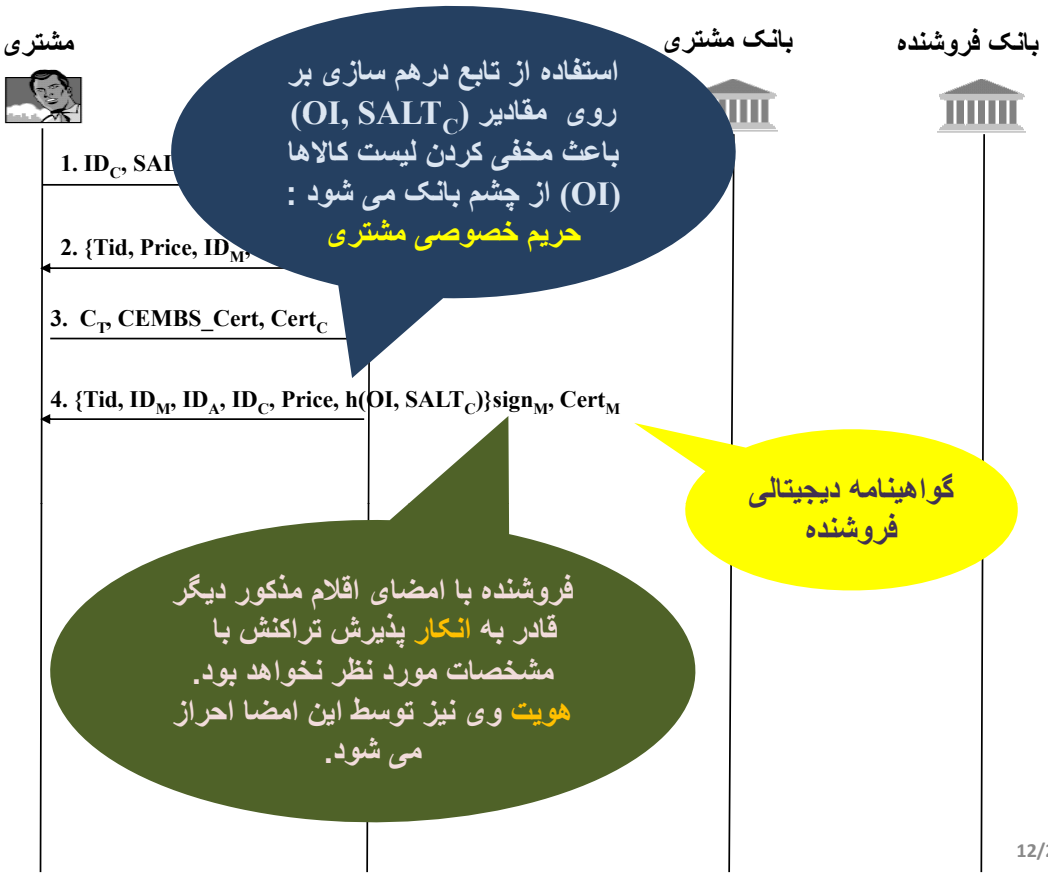
اطمینان مشتری از تطابق کالای رمز شده با توصیف مربوط به آن

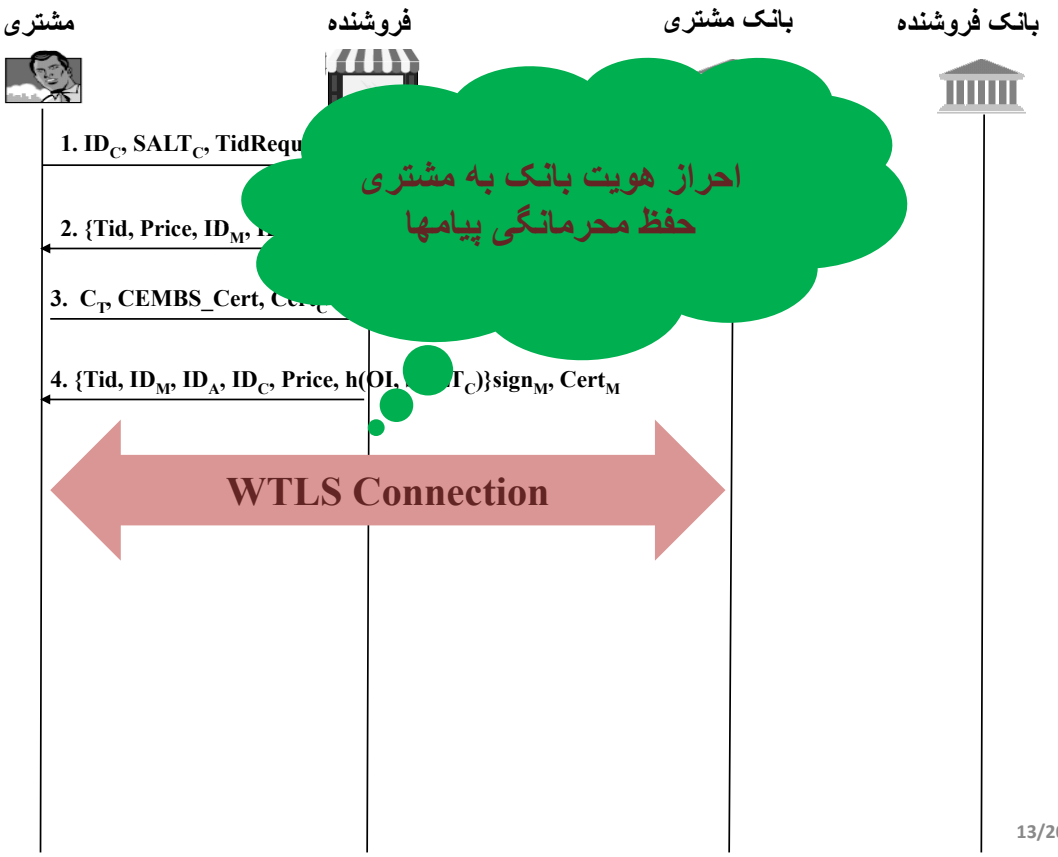


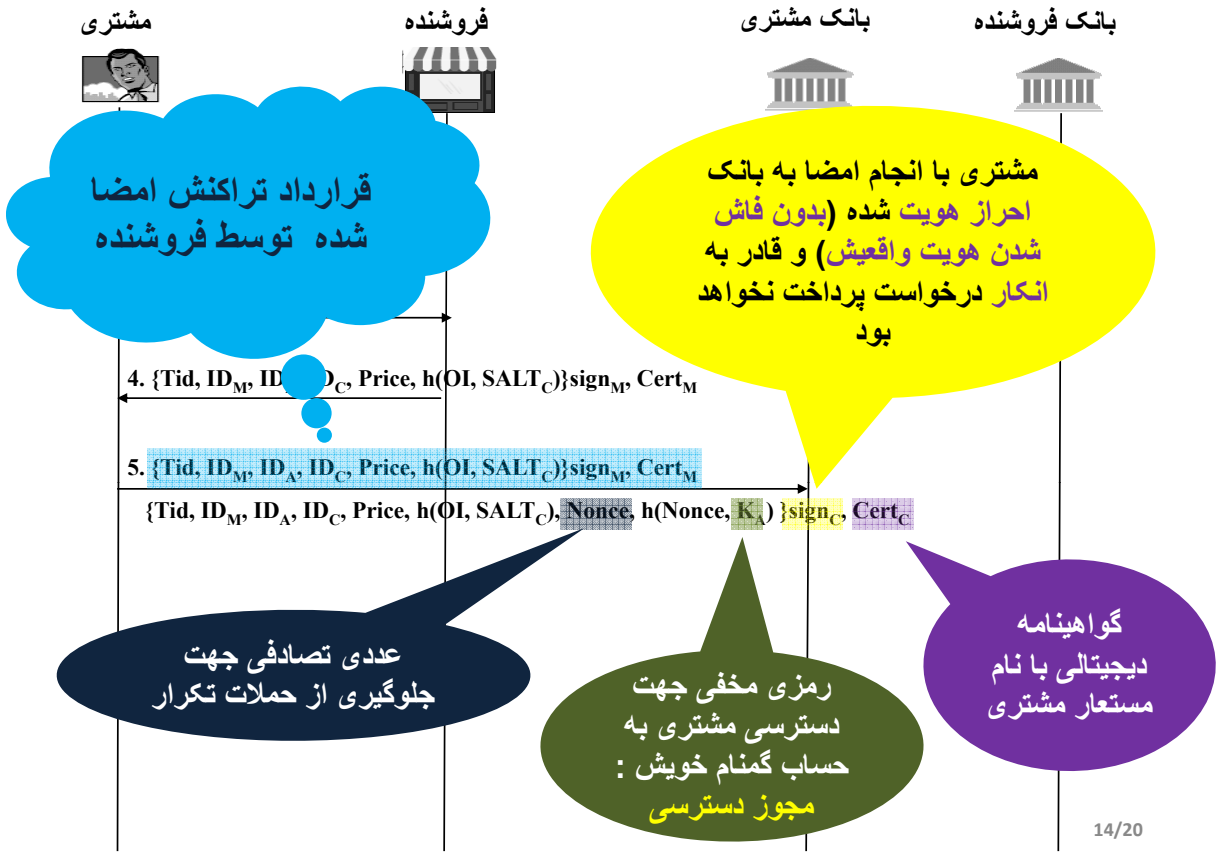

مشتری
فروشنده
بانک مشتری
بانک فروشنده
شناسه مشتری
Order Information
1. ID_C, $SALT_C$, TidRequest, OI
عددی تصادفی جهت مخفی کردن لیست کالاهای خرید از چشم بانک
درخواست ارسال یک شناسه منحصر به فرد برای تراکنش فعلی


شناسه تراکنش
فروشنده
بانک مشتری
بانک فروشنده
قیمت کالاها
ID_C, $SALT_C$
2. {Tid, Price, ID_M, ID_A} , [m , k]
شناسه فروشنده
شناسه بانک فروشنده
کالای رمز شده با کلید k که مشتری آن را با کالای دانلود شده از کاتالوگ مقایسه می کند : اطمینان از درستی کالا

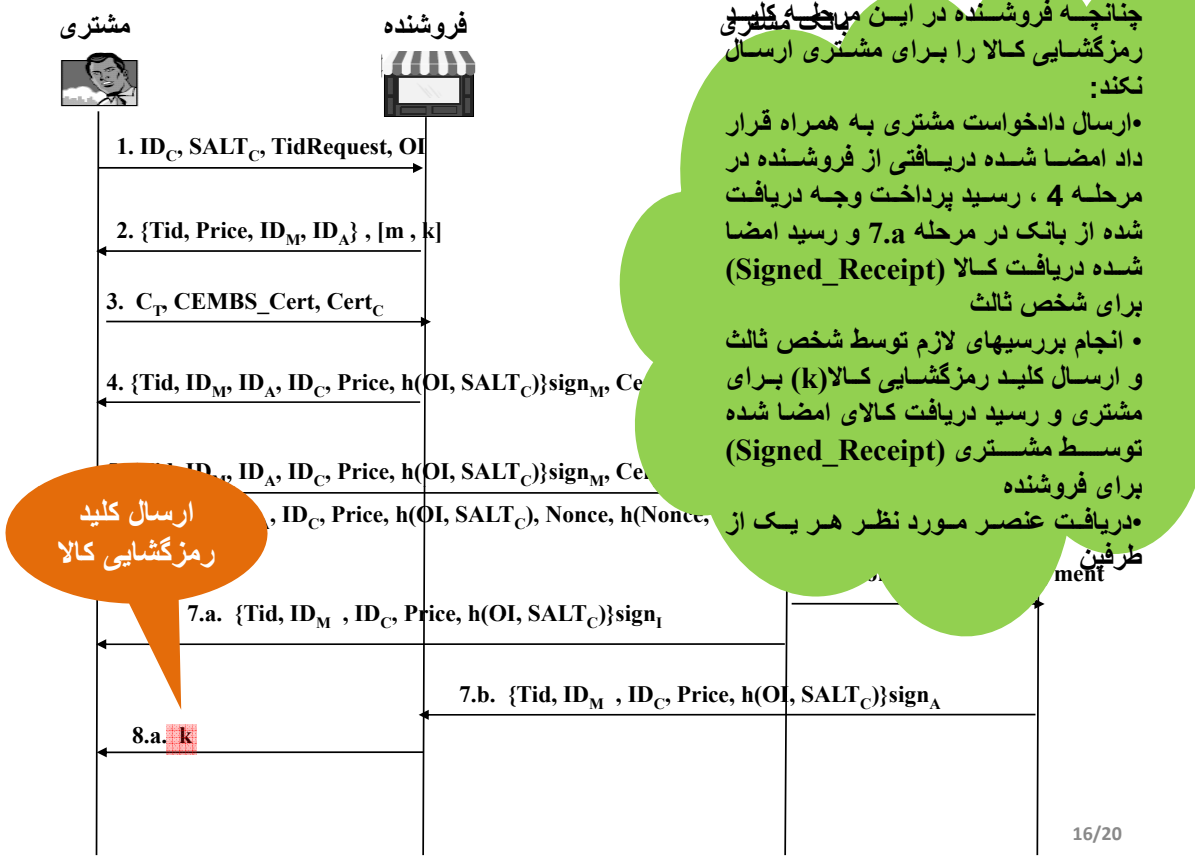

C_T = [Signed_Receipt, PK_T]
Signed_Receipt : {Tid, ID_M, ID_C, Price, OI}$Sign_C$
بانک فروشنده
2. {Tid. ... ID_M, ID_A} , [m , k]
3. C_T, CEMBS_Cert, $Cert_C$
CE توسط مشتری :
بدون آشکار کردن
اثبات می کند که C_T شامل
Sرمزنگاری شده با کلید
(PK_T) می باشد.)
این مرحله فروشنده را از دریافت رسید امضا شده مشتری در ازای تحویل کالا، مطمئن می سازد.

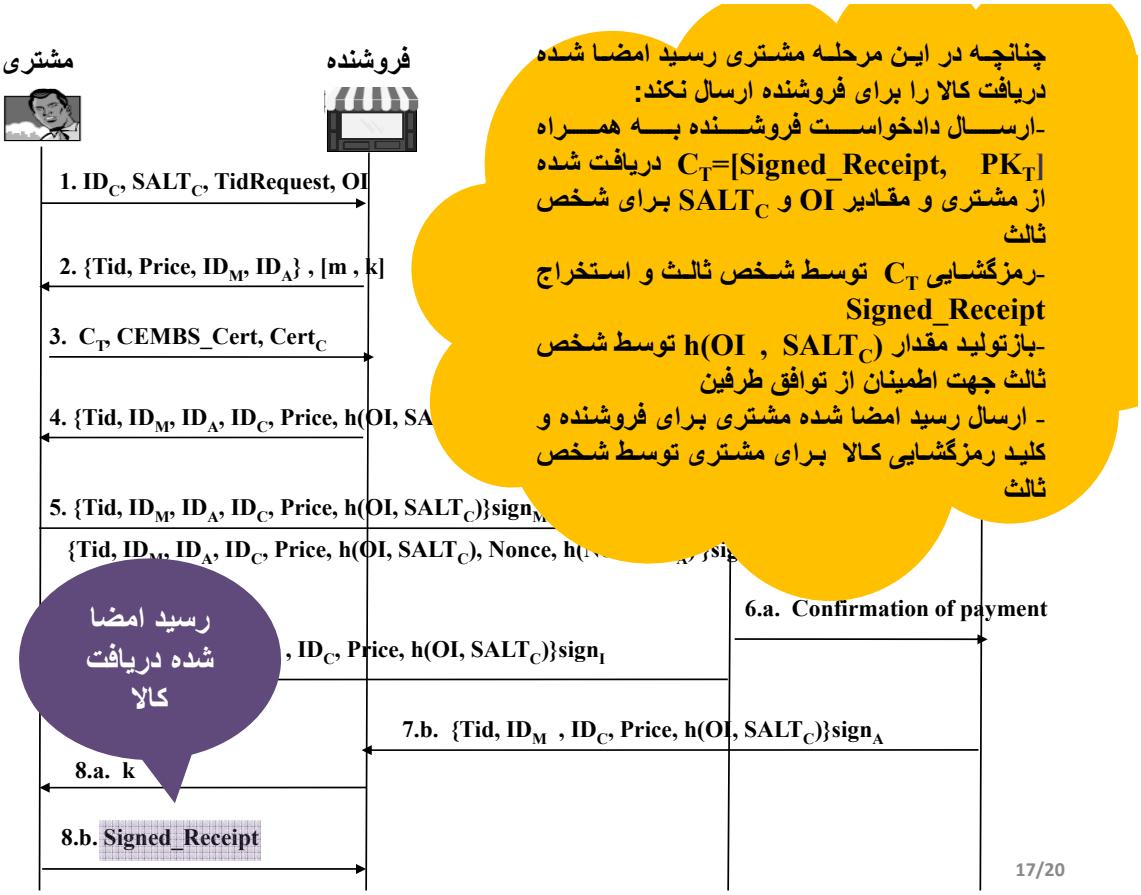

مشتری
بانک مشتری
بانک فروشنده
استفاده از تابع درهم سازی بر روی مقادیر ($OI, SALT_C$) باعث مخفی کردن لیست کالاها (OI) از چشم بانک می شود :
حریم خصوصی مشتری
1. ID_C, SAL
2. {Tid, Price, ID_M,
3. C_T, CEMBS_Cert, $Cert_C$
4. {Tid, ID_M, ID_A, ID_C, Price, h(OI, $SALT_C$)}$sign_M$, $Cert_M$
گواهینامه دیجیتالی فروشنده
فروشنده با امضای اقلام مذکور دیگر قادر به انکار پذیرش تراکنش با مشخصات مورد نظر نخواهد بود.
هویت وی نیز توسط این امضا احراز می شود.


مشتری
فروشنده
بانک مشتری
بانک فروشنده
1. ID_C, $SALT_C$, TidRequ
2. {Tid, Price, ID_M,
3. C_T, CEMBS_Cert,
4. {Tid, ID_M, ID_A, ID_C, Price, h(OI, T_C)}$sign_M$, $Cert_M$
احراز هویت بانک به مشتری
حفظ محرمانگی پیامها
WTLS Connection


مشتری
فروشنده
بانک مشتری
بانک فروشنده
قرارداد تراکنش امضا شده توسط فروشنده
مشتری با انجام امضا به بانک احراز هویت شده (بدون فاش شدن هویت واقعیش) و قادر به انکار درخواست پرداخت نخواهد بود
4. {Tid, ID_M, ID$_C$, Price, h(OI, $SALT_C$)}$sign_M$, $Cert_M$
5. {Tid, ID_M, ID_A, ID_C, Price, h(OI, $SALT_C$)}$sign_M$, $Cert_M$
{Tid, ID_M, ID_A, ID_C, Price, h(OI, $SALT_C$), Nonce, h(Nonce, K_A) }$sign_C$, $Cert_C$
عددی تصادفی جهت جلوگیری از حملات تکرار
رمزی مخفی جهت دسترسی مشتری به حساب گمنام خویش : مجوز دسترسی
گواهینامه دیجیتالی با نام مستعار مشتری


مشتری
فروشنده
بانک مشتری
بانک فروشنده
بانک امضای فروشنده و مشتری را تایید اعتبار و آنها را احراز هویت می کند. مقدار h(OI,SALT_C) ارسالی از دو طرف را مقایسه می کند تا مطمئن شود طرفین روی لیست کالا توافق دارند. K_A را از پایگاه اطلاعات خود ا... K ارسالی از مشتری مقایسه میکند. در... اخت را از حساب مشتری کاسته ... ه را به بانک
دریافت رسید پرداخت وجه امضا شده توسط بانک مشتری: عدم امکان انکار پرداخت وجه توسط مشتری
دریافت رسید پرداخت وجه امضا شده توسط بانک فروشنده : اطمینان فروشنده از دریافت وجه
4. {Tid,
5. {Tid, ID_M, ID_A, ID_C, Price,
{Tid, ID_M, ID_A, ID_C, Price, h(OI, SALT_C), N... Nonce, K_A) }sig...
6.a. Not...
7.a. {Tid, ID_M , ID_C, Price, h(OI, SALT_C)}sign_I
7.b. {Tid, ID_M , ID_C, Price, h(OI, SALT_C)}sign_A


مشتری
فروشنده
بانک مشتری
چنانچه فروشنده در این مرحله کلید رمزگشایی کالا را برای مشتری ارسال نکند:
•ارسال دادخواست مشتری به همراه قرار داد امضا شده دریافتی از فروشنده در مرحله 4 ، رسید پرداخت وجه دریافت شده از بانک در مرحله 7.a و رسید امضا شده دریافت کالا (Signed_Receipt) برای شخص ثالث
• انجام بررسیهای لازم توسط شخص ثالث و ارسال کلید رمزگشایی کالا(k) برای مشتری و رسید دریافت کالای امضا شده توسط مشتری (Signed_Receipt) برای فروشنده
•دریافت عنصر مورد نظر هر یک از طرفین
ارسال کلید رمزگشایی کالا
1. ID_C, SALT_C, TidRequest, OI
2. {Tid, Price, ID_M, ID_A} , [m , k]
3. C_T, CEMBS_Cert, Cert_C
4. {Tid, ID_M, ID_A, ID_C, Price, h(OI, SALT_C)}sign_M, Ce...
..., ID_A, ID_C, Price, h(OI, SALT_C)}sign_M, Ce...
..., ID_C, Price, h(OI, SALT_C), Nonce, h(Nonce,
ment
7.a. {Tid, ID_M , ID_C, Price, h(OI, SALT_C)}sign_I
7.b. {Tid, ID_M , ID_C, Price, h(OI, SALT_C)}sign_A
8.a. k



مقایسه ویژگیهای امنیتی پروتکلها

پروتکل / ویژگی امنیتی	NetBill	Lee's	FAPSWPP
محرمانگی	بله	بله	بله
احراز هویت	بله	بله	بله
جامعیت داده	بله	بله	بله
انکارناپذیری تراکنش توسط فروشنده	بله	-	بله
انکارناپذیری تراکنش توسط مشتری	بله	-	بله
انکار ناپذیری دریافت وجه توسط فروشنده	-	بله	بله
حفظ حریم خصوصی	-	بله	بله
گمنامی مشتری	-	-	بله
اطمینان مشتری از دریافت کالا در ازای پرداخت وجه	بله	-	بله
اطمینان فروشنده از دریافت وجه در ازای تحویل کالا	بله	بله	بله
اطمینان فروشنده از دریافت رسید تحویل کالا	-	-	بله

مقایسه ویژگیهای کارایی پروتکلها

بهبود کارایی

بهبود کارایی

نام پروتکل / معیار کارایی	Lee' s et al	NetBill	FAPSWPP
Public-key Enc/ Dec	8	6	1
Digital signature/ verification	9	13	10
Symmetric operation	2	28	2
Hash function (*H*)	9	2	4
CEMBS Generation/ Verification	0	0	2
Communication overhead (number of messages)	9	15	10

با تشکر از توجه شما

شهریور 1390