پرداخت

احراز هویت

# امضای همراه
# Mobile )
# (Signature

امضا

# موضوعات

- نیاز
- بازیگران اصلی
  - فراهم‌کنندگان خدمات آنلاین
  - اپراتورهای تلفن همراه
  - دولت و حاکمیت
- مروری اجمالی بر مفاهیم استانداردهای امضا با موبایل ( ETSI MSS)
- چگونگی ایفای نقش کلیدی توسط سیم‌کارت و زیرساخت شبکه‌ای اپراتور
- چگونگی بکارگیری توسط کاربر

# ذی‌نفعان کلیدی

- فراهم‌کننده خدمات آنلاین
  - خدماتی نظیر پرداخت و بانکداری اینترنتی
  - پایگاه‌های ارائه خدمات به مشتریان

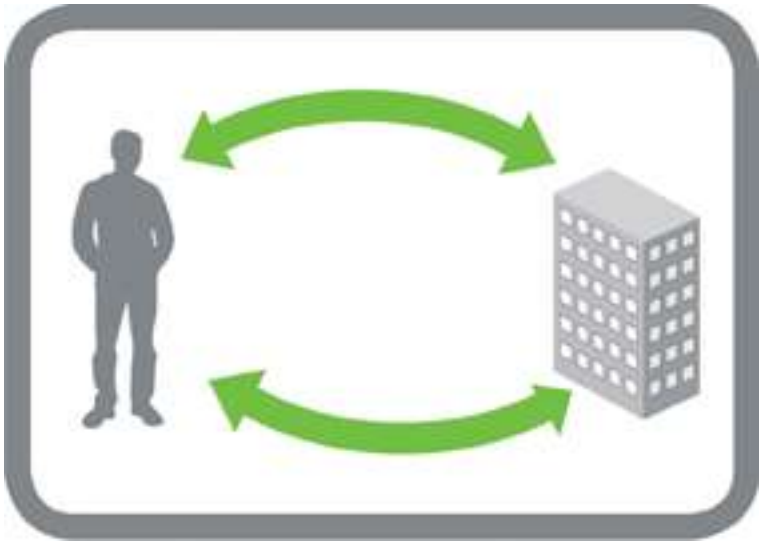
- اپراتور تلفن همراه
  - زیرساخت شبکه
  - مشترکین
- دولت و حاکمیت
  - خدمات همگانی بیش از پیش مبتنی بر وب خواهد شد.
  - احراز هویت به شکل دو عامله، مبتنی بر امضای الکترونیکی و با استفاده از تلفن همراه افراد انجام خواهد شد.

- مشتری
  - کاربرانی که از ارزش‌های افزوده بهره می‌گیرند.

# فراهم‌کنندگان خدمات آنلاین
## (نیازها و محرک‌های کلید)

# محرک‌های کلیدی فراهم‌کننده خدمات آنلاین

- احراز هویت از طریق کانالی مجزا از کانال ارائه خدمت
- غیر ممکن سازی حملاتی نظیر مرد میانی و یا فیشینگ و ...



# محرک‌های کلیدی فراهم‌کننده خدمات آنلاین

- توافقات قانونی الزام‌آور از طریق بکارگیری تلفن همراه
- انکارناپذیری توافقات

# تحلیلی بر روش‌های مختلف امنیتی

| | لیست PIN/TAN | توکن رمز یک‌بار مصرف | رمز یک‌بار مصرف از طریق پیامک | امضای همراه |
|---|---|---|---|---|
| |  |  |  |  |
| **ابزار مورد نیاز** | لیست‌های متفاوت که از طریق فراهم‌کنندگان کاربرد، مدیریت و صادر می‌گردد. | چند توکن که هر کدام توسط یک فراهم‌کننده کاربرد، مدیریت می‌گردد. | یک گوشی تلفن همراه معمولی | یک گوشی تلفن همراه که از طریق یک سیم‌کارت هوشمند و یا به روشی دیگر، از زیرساخت کلید عمومی پشتیبانی کند. |
| **قابلیت بکارگیری در چند کاربرد مختلف** | فقط قابل استفاده در حوزه خدمات کاربردی فراهم‌کننده مربوطه | فقط قابل استفاده در حوزه خدمات کاربردی فراهم‌کننده مربوطه | کلیه کاربردها | کلیه کاربردها |
| **عملیاتی که شهروند می‌بایست انجام دهد.** | وارد نمودن مجدد کد رمز جدید برای هر بار استفاده به صورت دستی در پایانه | وارد نمودن مجدد کد رمز جدید برای هر بار استفاده به صورت دستی در پایانه | وارد نمودن مجدد کد رمز جدید برای هر بار استفاده به صورت دستی در پایانه | وارد نمودن رمز شخصی در تلفن همراه |
| **نیازمندی‌های قابل حمل** | لیست رمزهای عبور (تک منظوره) | یست رمزهای عبور (تک منظوره) | تلفن همراه | تلفن همراه |
| **هزینه خدمات پشتیبانی مشتری** | بر عهده فراهم کننده کاربرد است. | بر عهده فراهم کننده کاربرد است. | بر عهده اپراتور تلفن همراه است. | بر عهده اپراتور تلفن همراه است. |
| **محدودیت‌های بکارگیری** | قابل کپی‌برداری و نیازمند صدور مجدد است. حملات فیشینگ و مرد میانی | تمام شدن باطری، به‌روزرسانی پین‌کدها، سایر مسائل پشتیبانی | دسترسی به شبکه تلفن همراه | دسترسی به شبکه تلفن همراه، معتبر بودن گواهی الکترونیکی مورد استفاده، پشتیبانی سیم‌کارت یا تلفن همراه از زیرساخت کلید عمومی |
| **هزینه‌های گسترش** | هزینه‌های مداوم و تکراری (تک منظوره) | گران (تک منظوره) | بدون هزینه | تمدید یا صدور مجدد گواهی الکترونیکی که معمولاً به صورت سالانه انجام می‌شود. |

# مقایسه روش‌های مختلف احراز هویت بر اساس هزینه

| روش احراز هویت | لیست PIN/ TAN | رمز یکبار مصرف | امضا بر روی موبایل | توکن سخت‌افزاری | توکن نرم‌افزاری | کارت هوشمند |
|---|---|---|---|---|---|---|
| هزینه استفاده در سال | 13 € | 15 € | **12 €** | 35 € | 50 € | 100 € |
| قابلیت بکارگیری | LOW | MEDIUM | **HIGH** | LOW | MEDIUM | LOW |

Source: Entrust and MSS business model security cost analyze, 10000 users, 3 year period

# منافع فراهم‌کننده خدمات آنلاین

- افزایش سطح امنیتی
  - امنیت دو عامله
- کاهش هزینه‌ها
  - عدم وابستگی به وجود یک توکن یا کارت هوشمند
  - نیاز کمتر به صرف هزینه‌های مدیریت و نگهداری
  - ارتقای خدمات از طریق کاهش هزینه تراکنش‌ها
- ایجاد ظرفیت جهت بازگشت بیشتر سرمایه
  - خدمات ارزش افزوده
  - کنترل مجوز برای نهادهای ثالث
- افزایش سهولت برای مشتریان
  - افزایش ضریب نفوذ موبایل
  - سادگی تعامل برای کاربر

- کانال مشترک
  - یک روش مشترک احراز هویت برای کلیه نقاط دسترسی، مانند اینترنت، موبایل، تلویزیون دیجیتال و ...
- تراکنش‌های مشترک
  - یک روش مشترک برای انجام انواع مختلف تراکنش‌ها، مانند ورود به سیستم، پرداخت، گردش کار، تاییدیه، امضا و ...
- امنیت برای همه بخش‌ها
  - شناسایی مشتریان
  - شناسایی فراهم‌کنندگان خدمات آنلاین
  - حفظ محرمانگی
  - عدم امکان انکار یک تراکنش

# اپراتور تلفن همراه

# نیازها

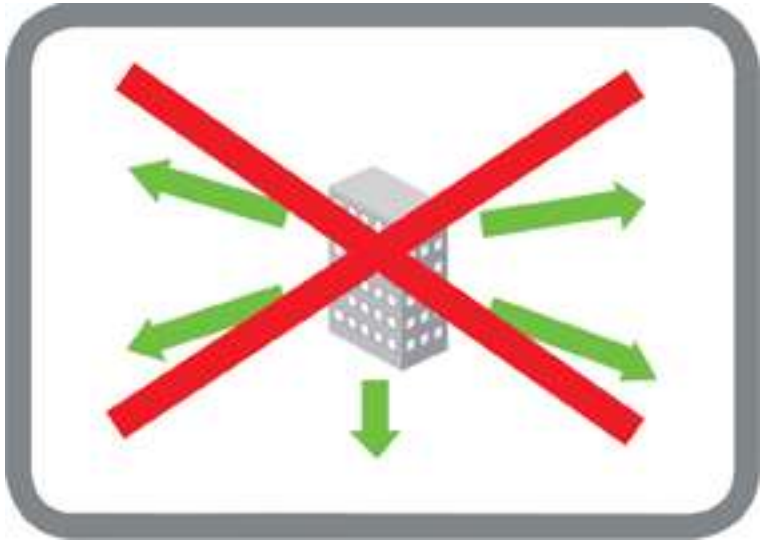
- اپراتورها پس از سرمایه‌گذاری‌های سنگینی که در سال‌های اخیر جهت توسعه شبکه، رقابت و نیز ارتقای نسل، مانند استقرار تلفن همراه نسل سوم، عمیقا نیاز به جریان بازگشت سرمایه دارند.
- ابتکار و نوآوری در خلق خدمات ارزش افزوده تنها راه ایجاد این جریان است.
- خدمات باید یک بازار انبوه را پشتیبانی کنند. بطور مثال حوزه حاکمیتی و حوزه مال و اقتصادی
- گاهی اوقات، انتقال و یا تغییر تعدادی زیادی شماره تلفن ممکن است باعث ایجاد یک دردسر بزگ شود.

# محرک‌های کلیدی

- امکان ارائه طیف گسترده‌ای از سرویس‌های امنیتی
- مشتریان تجاری و مصرف‌کننده

# محرک‌های کلیدی

- یک سیم‌کارت که بر روی آن گواهی الکترونیکی و کلیـد نصـب شده باشد، باعث کاهش احتمال تغییر اپراتور تلفن همراه توسط مشتری می‌شود.



# Mobile PKI

- زیرساخت کلید عمومی راه‌حل فنی ایده‌آل رفع این نیاز است.
- هر کس یک تلفن همراه (سیم‌کارت) دارد.
- بنابراین پیاده‌سازی زیرساخت کلید عمومی روی سیم‌کارت راه‌حل ایده‌آل است.
- زیرساخت کلید عمومی بر روی موبایل با عنـوان Mobile PKI و یا Wireless PKI شناخته شده است.
- Mobile PKI تنها یک توانمند سـاز بـرای ایـن گونـه خـدمات است.

# دولت و حاکمیت

# محرک‌های کلیدی

- هرگونه خدمات شهروندی قابل ارائه توسط دولت ممکن است بتواند از طریق وب ارائه شود.
- هر سرویسی که شامل اطلاعات حساس باشد (مالی، سلامت و ...) نیازمند یک شیوه احراز هویت مستحکم است.
- بطور مثال کارت ملی شهروندی افراد می‌تواند مبتنی بر PKI باشد.

# تجربه‌های موفق در اروپا

- 2006 Manchester Declaration, setting objectives for a EU eIDM interoperability and mutual recognition of national eIDM
- 2007 Common spesifications for interoperable EIDM and call for large scale pilots
- 2008 Large scale pilots of eIDM in cross-border services
- 2009 eSignatures in eGovernment, undertake review of take-up in public services
- 2010 Review the uptake by the Member States, interoperable eIDM at work

Countries in piloting phase:

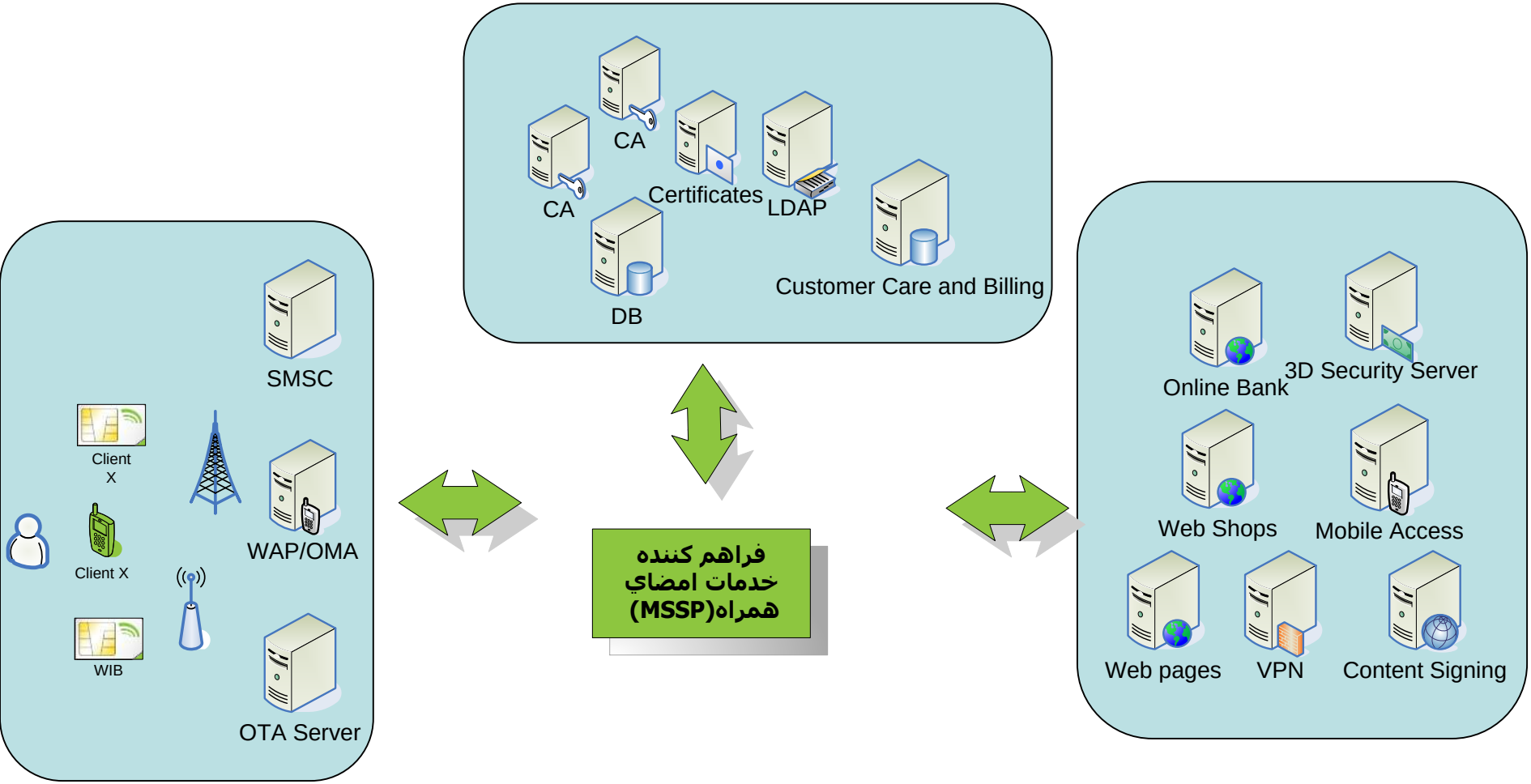
Austria/Belgium (leading countries), UK, Germany, Italy, Poland, Netherlands, Portugal, Malta, Estonia + possibly others

# راه‌حل Mobile PKI

# Mobile PKI

- در سال ۲۰۰۰ هنوز هیچ استانداردی در این زمینه وجود نداشت.
- اولین بار در سال ۲۰۰۲، موسسه استانداردهای مخابراتی اروپا (ETSI)، استانداردهایی نظیر استانداردهای زیر منتشر شد:
  - ETSI TR 102 203 (نیازمندی‌های کسب و کار و عملیاتی)
  - ETSI TR 102 206 (چارچوب امنیتی)
  - ETSI TS 102 207 (رومینگ)
  - ETSI TS 102 204 (واسط وب)
  - ETSI TS 100 977 (خصوصیات واسط سیم‌کارت)
  - ETSI SR 002 176 (الگوریتم و پارمترهای امضای الکترونیکی)
  - ETSI TS 131 130 (واسط برنامه‌نویسی سیم‌کارت)
  - و ...
- در حال حاضر کلیه راه‌حل‌های پیاده‌سازی شده، خود را بر اساس استانداردهای ETSI ارتقا داده‌اند.

# Mobile PKI / MSS



# سهولت و سادگی احراز هویت


- تمام چیزی که برای احراز هویت خود نیاز دارید عبارت است از یک عدد سیم‌کارت!

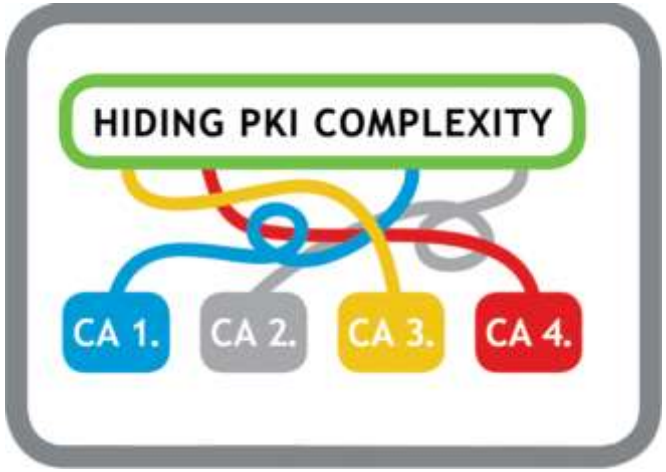


# الزام‌آوری قانونی

- انجام توافقات قانونی از طریق تلفن همراه
- انکارناپذیری
- شناسایی رسمی اشخاص حقیقی و حقوقی

# پنهان‌سازی پیچیدگی‌های PKI

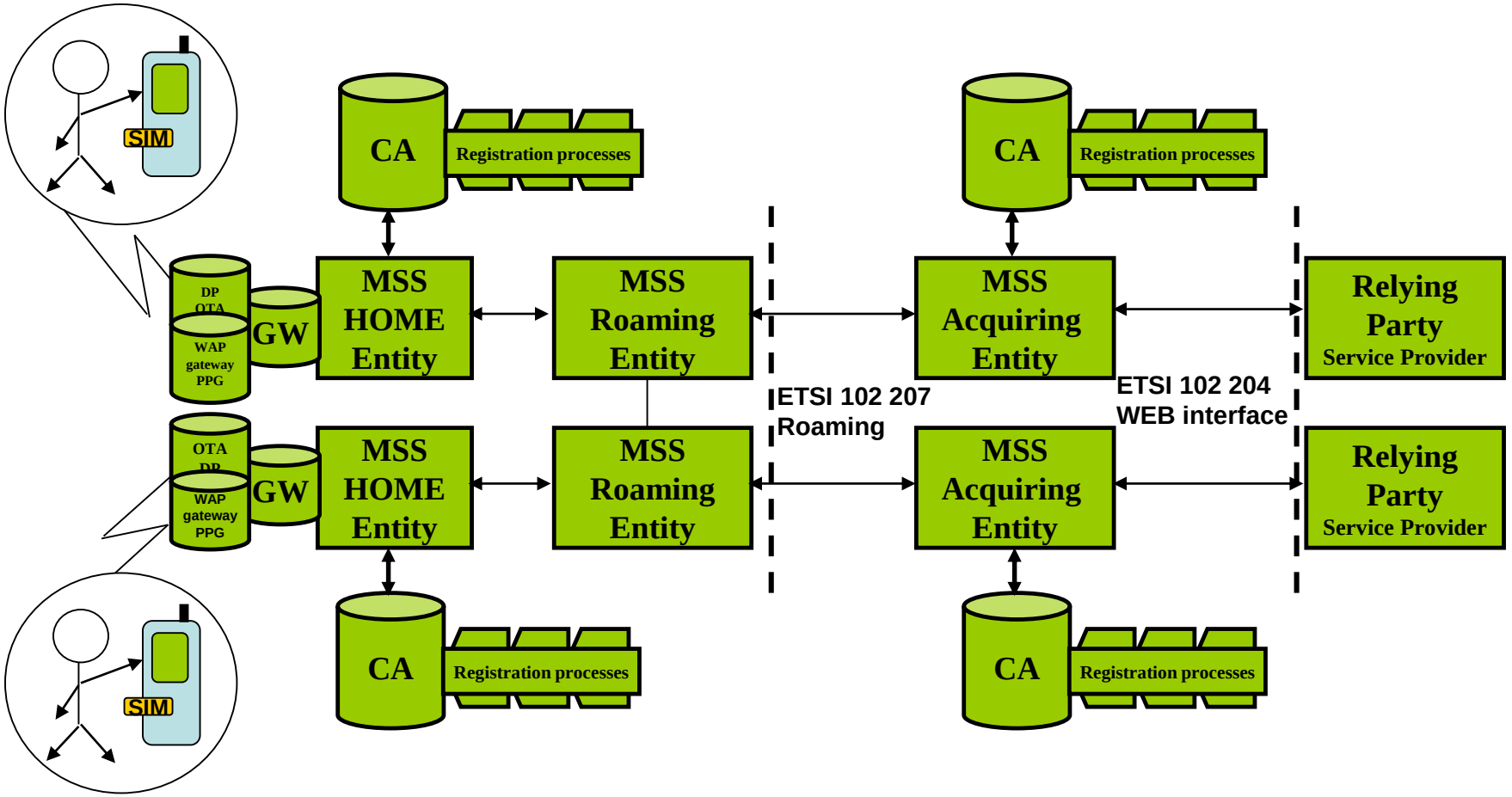
- پشتیبانی از چندین CA و زیرساخت کلید عمومی مختلف بصورت همزمان
- عدم نیاز به هیچ فناوری یا سیاست‌گذاری



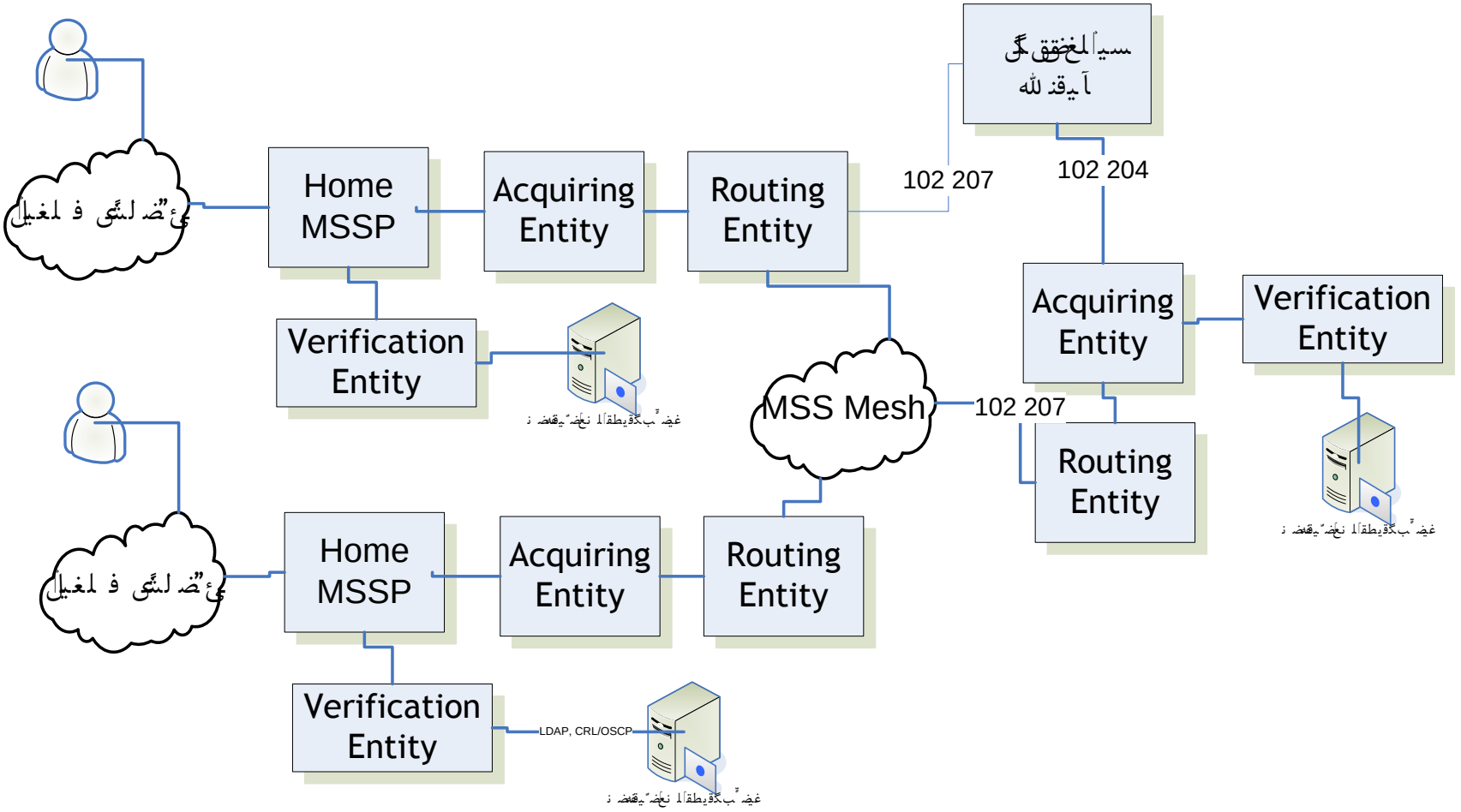
# ETSI MSS

- استانداردهای فراهم‌کننده خدمات امضای موبایل (ETSI MSSP) مبتنی بر چهار موجودیت زیر است:
  - Home Entity (به یک کلاینت مجزا و اختصاصی اختصاص دارد)
  - Acquiring Entity (بدست آورنده امضا)
  - Routing Entity (فراهم‌کننده رومینگ در بین شبکه های اپراتورهای مختلف)
  - Verification Entity (که ممکن است با با موجودیت اول یا دوم ادغام شود.)
- هر یک از این موجودیت‌ها می‌توانند با هم ادغام شوند و یا بصورت مجزا پیاده‌سازی شوند.
- استانداردهای ETSI در برگیرنده واسط‌های بین موجودیت‌ها و برای یکپارچه‌سازی هر کاربردی که از امضا بر روی موبایل استفاده می‌کند، هستند.

# خصوصیات نقش‌ها در استاندارد ETSI 102

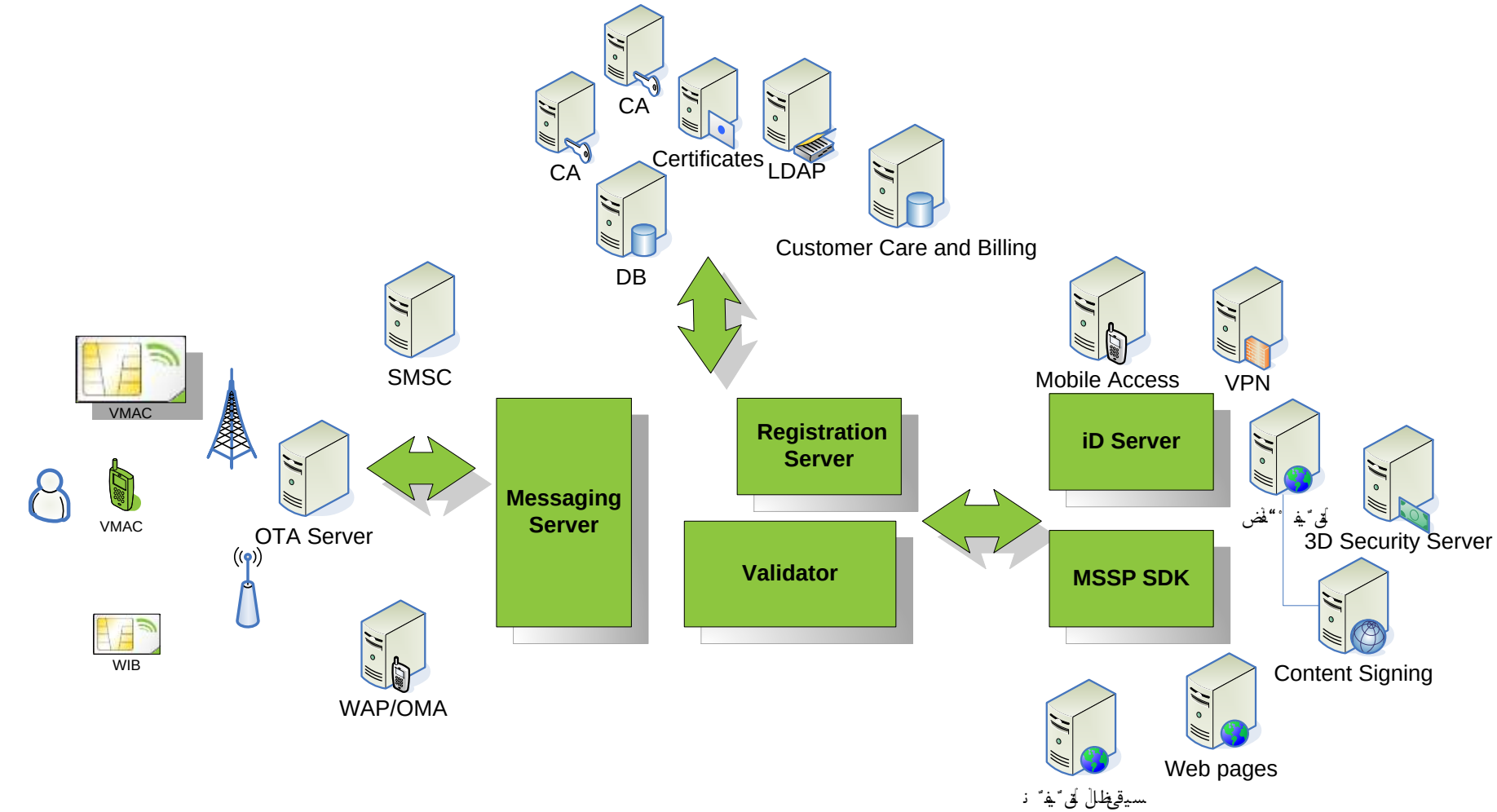


# رومینگ امضا در MSSP



# نقش کلیدی اپراتورهای تلفن همراه

# راه حل زیربنایی



# نقش کلیدی اپراتورهای تلفن همراه

- همه چیز از سیم‌کارت، جایی که زوج‌کلیدها و Hash امضا در یک فضای حفاظت شده نگهداری می‌شوند، شروع می‌شود.
- از نظر فنی تنها اپراتورهای تلفن همراه می‌توانند مجوز دسترسی به سیم‌کارت‌ها را داشته باشند.
- البته سازندگان تلفن همراه نیز می‌توانند یک فضای محافظت شده‌ای را در قالب یک تراشه فراهم کنند تا از آن جهت نگهداری زوج‌کلید استفاده شود. اما این در دنیا به دلایل تجاری مرسوم نشده است.


# صدور گواهی و زوج‌کلید

- تراشه داخل سیم‌کارت دربرگیرنده کلید خصوصی معمولا توسط اپراتور تلفن همراه صادر می‌شود.
- هویت مالک سیم‌کارت بر اساس اطلاعات گواهی وی که در مراکز صدور گواهی ثبت شده است، تعیین می‌گردد.
- گواهی‌های الکترونیکی بر روی سیم‌کارت قرار نمی‌گیرند. بلکه از طریق مخزن مرکز صدور گواهی منتشر می‌شوند.

# تجربه Mobile PKI
# در بانکداری الکترونیک

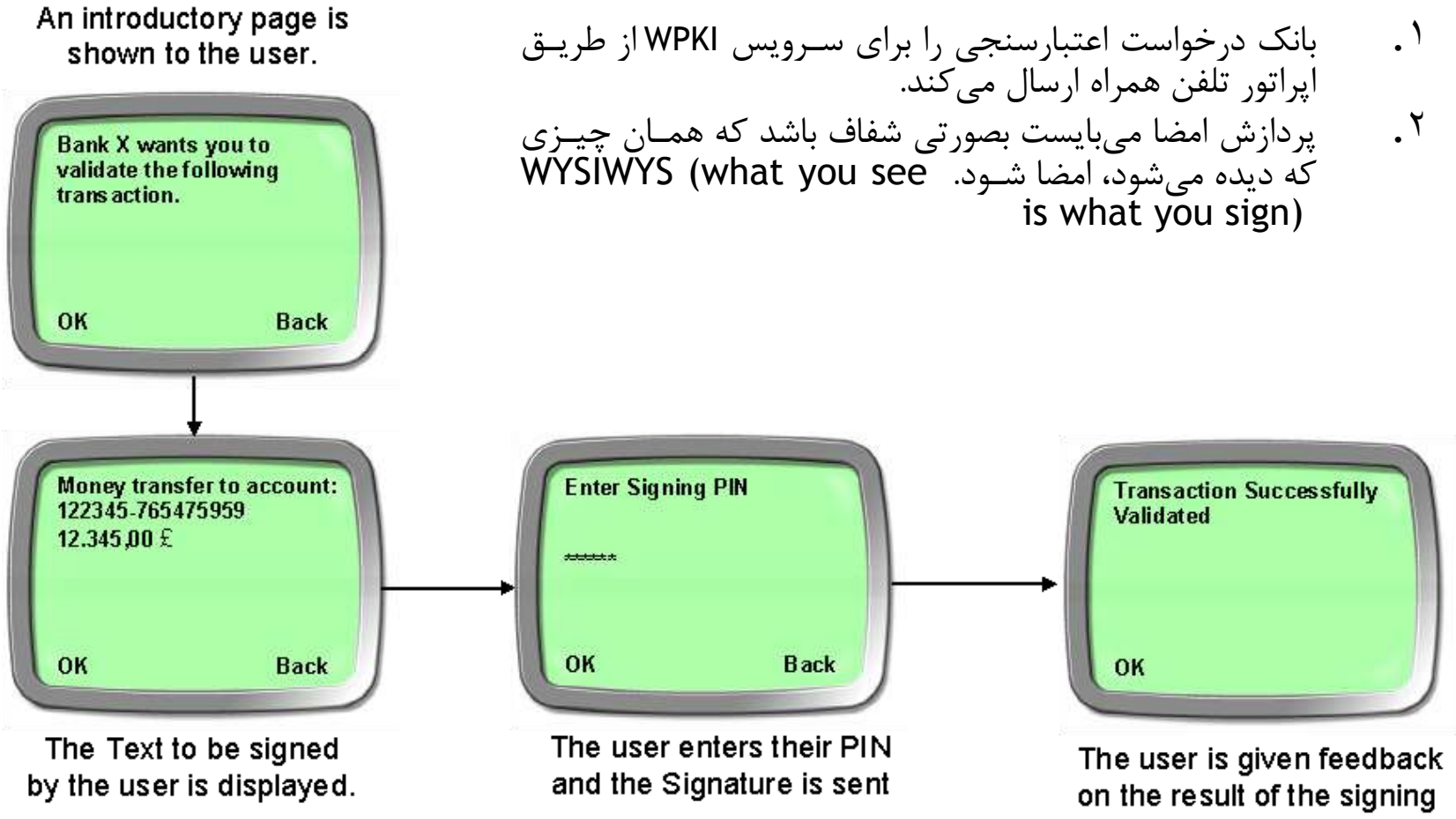
# احراز هویت در بانکداری الکترونیکی

۱. کاربر نهایی با نام کاربری خود به سایت بانک مراجعه می‌کند.
۲. سیستم بانک یک درخواست احراز هویت را بر اساس شماره تلفن همراه کاربر بـرای WPKI از طریـق اپراتـور تلفن همراه ارسال می‌کند.
۳. کاربر پین‌کد را در تلفن همراه خود وارد می‌کند.
۴. به کاربر اجازه ورود به سایت بانک داده می‌شود.

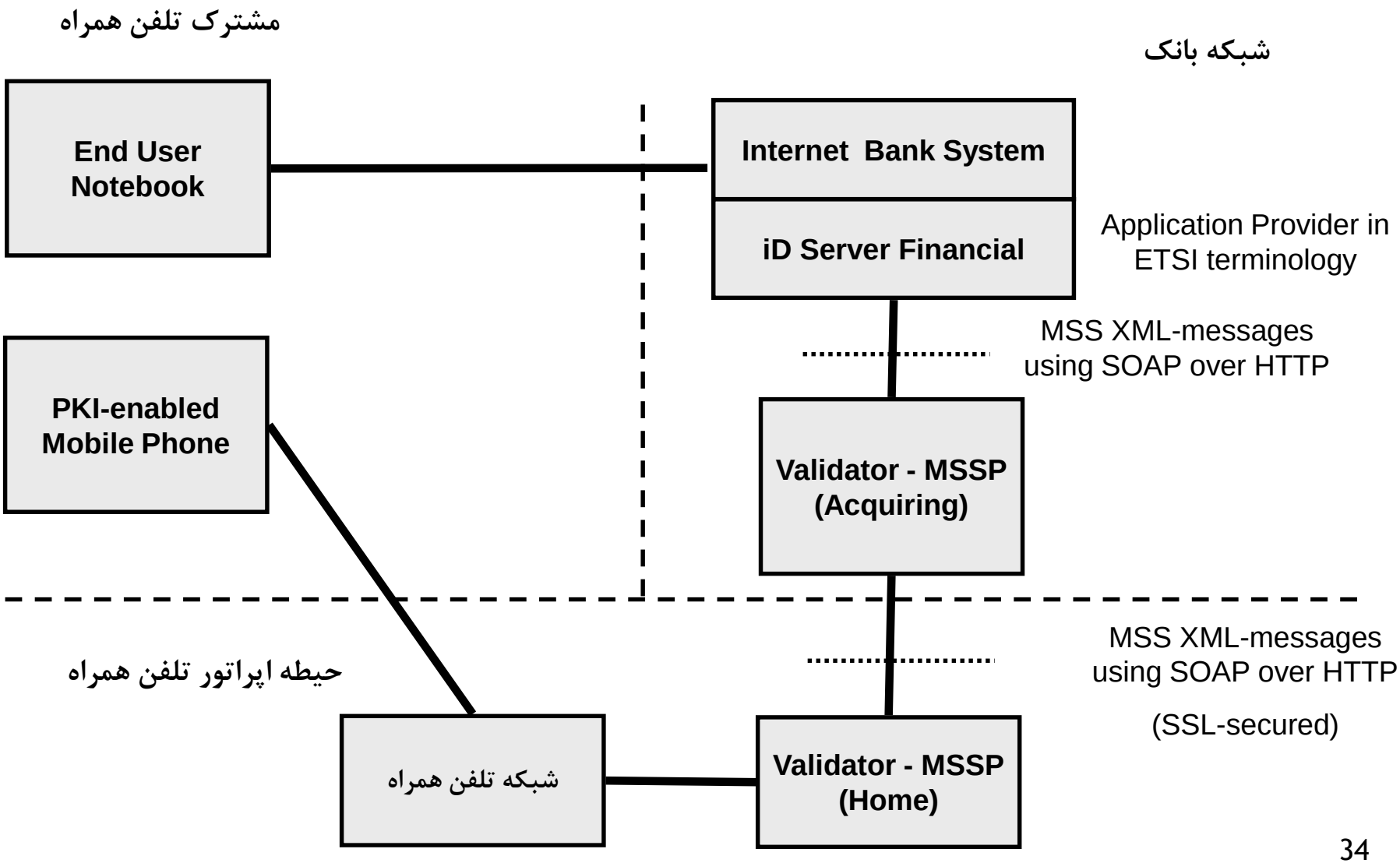
# اعتبارسنجی تراکنش در بانکداری الکترونیکی

۱. بانک درخواست اعتبارسنجی را برای سـرویس WPKI از طریـق اپراتور تلفن همراه ارسال می‌کند.

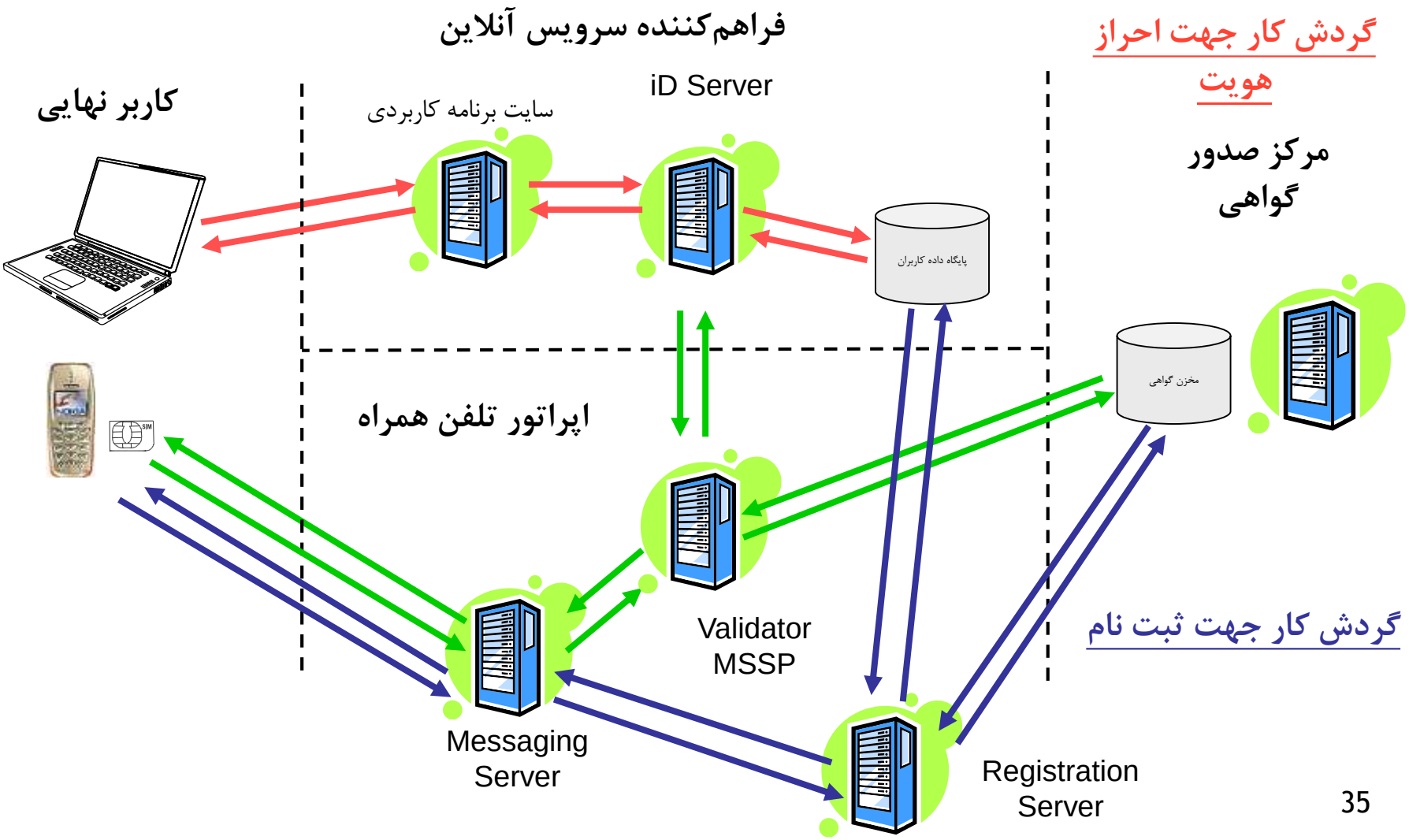
۲. پردازش امضا می‌بایست بصورتی شفاف باشد که همـان چیـزی که دیده می‌شود، امضا شـود. WYSIWYS (what you see is what you sign)



# یک سناریو جهت راه‌اندازی زیرساخت



# مدل گردش کار بین موجودیت‌ها



تلفن همراه یک وسیله مطمئن است که

در **هرجا** و **هر وقت** جهت دسترسی به اطلاعات تجاری، اعتباری و شخصی قابل استفاده است.

# با سپاس