



# فصل چهارم: زیرساخت لایه عمومی

امنیت سیستم‌های کامپیوتری

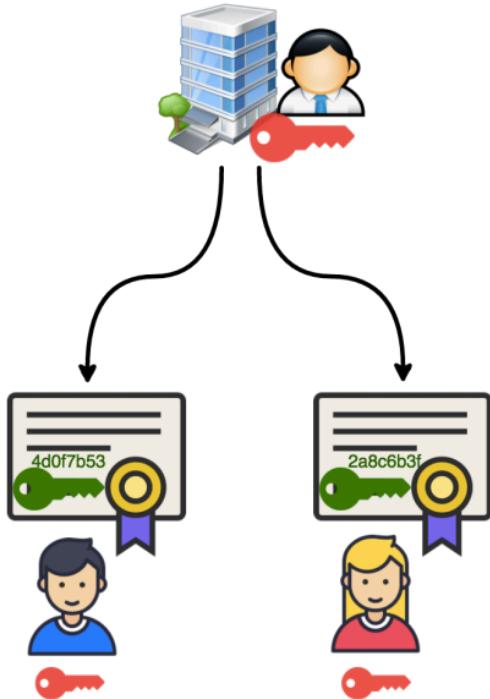
ابوالفضل دیانت

آخرین ویرایش: ۲۹ فروردین ۱۴۰۲ در ساعت ۱۱ و ۴۳ دقیقه - نسخه ۱.۰.۲

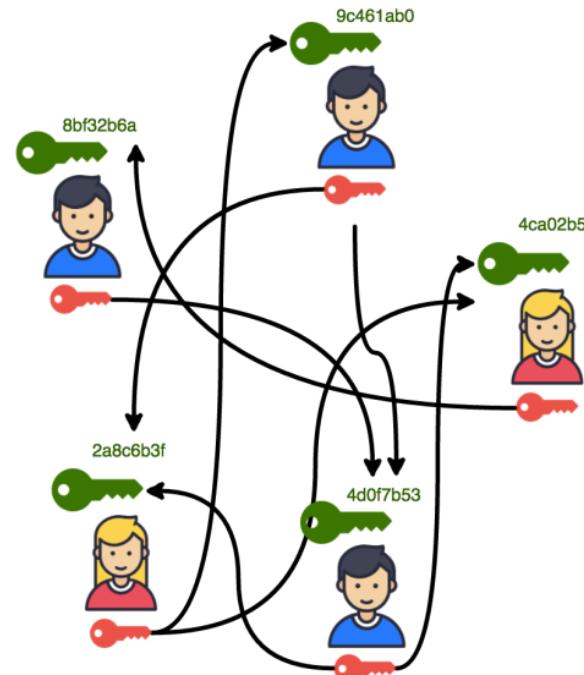
# مراجع صور، گواہینا مہ

# یک راه کار با دو رهیافت برای حل مشکل مردمیانی

## CERTIFICATE AUTHORITY



## PGP / WEB OF TRUST



- ☞ نیاز به یک گواهینامه به مانند گواهینامه ماشین و همچنین مرکز صدور گواهینامه.
- ☞ یک جایگزین برای CA، روشی غیر مرکز به نام وب اعتماد (Web of trust) است.

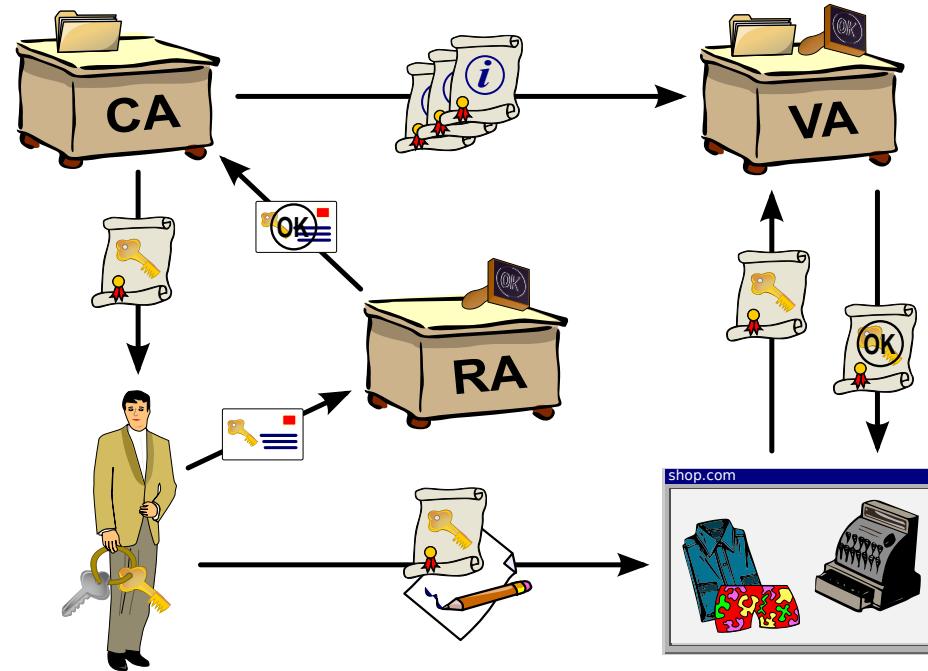
Alice می‌خواهد پیامی برای Bob ارسال کند. می‌دانید که کافی است تا Alice پیام را با کلید عمومی Bob رمز نموده و برای او ارسال نماید. در سوی دیگر، Bob نیز با کلید محرمانه خود، پیام را باز نماید. با کمی دقت می‌توان دریافت که پروتکل مذکور از چالش حمله مردمیانی (Man in the middle) است. چراکه Eve به عنوان یک حمله‌گر می‌تواند یک کلید عمومی ساختگی را به عنوان کلید عمومی Bob به Alice تحويل دهد. برای حل این مشکل باید چه کرد؟

یک ایده مناسب برای حل چالش بیان شده، استفاده از یک شخص ثالث قابل اطمینان است، که همه به آن اعتماد (Trust) دارند. انتظار ما این است که این شخص مورد اعتماد، به Bob یک گواهینامه بدهد. گواهینامه در یک بیان ساده، یک برگه است که در آن کلید عمومی Bob به همراه شناسه او و امضای شخص مورد اعتماد قرار دارد. هنگامی که این برگه در اختیار Alice قرار می‌گیرد، او امضای شخص مورد اعتماد را می‌شناسد، پس مطمئن می‌شود که محتوای برگه درست است. به نظر مشکل حل شد ...!

در روش دوم، به جای اتکا بر سلسله مراتبی از مراجع صدور گواهینامه، گواهینامه‌ها توسط سایر کاربران امضا

می‌شوند تا این تضمین ایجاد شود که کلید عمومی ذکر شده، مربوط به فرد یا نهاد لیست شده در مجوز است. این مفهوم در نرم‌افزار رمزگذاری PGP (Pretty Good Privacy) استفاده می‌شود.

# PKI چیست؟

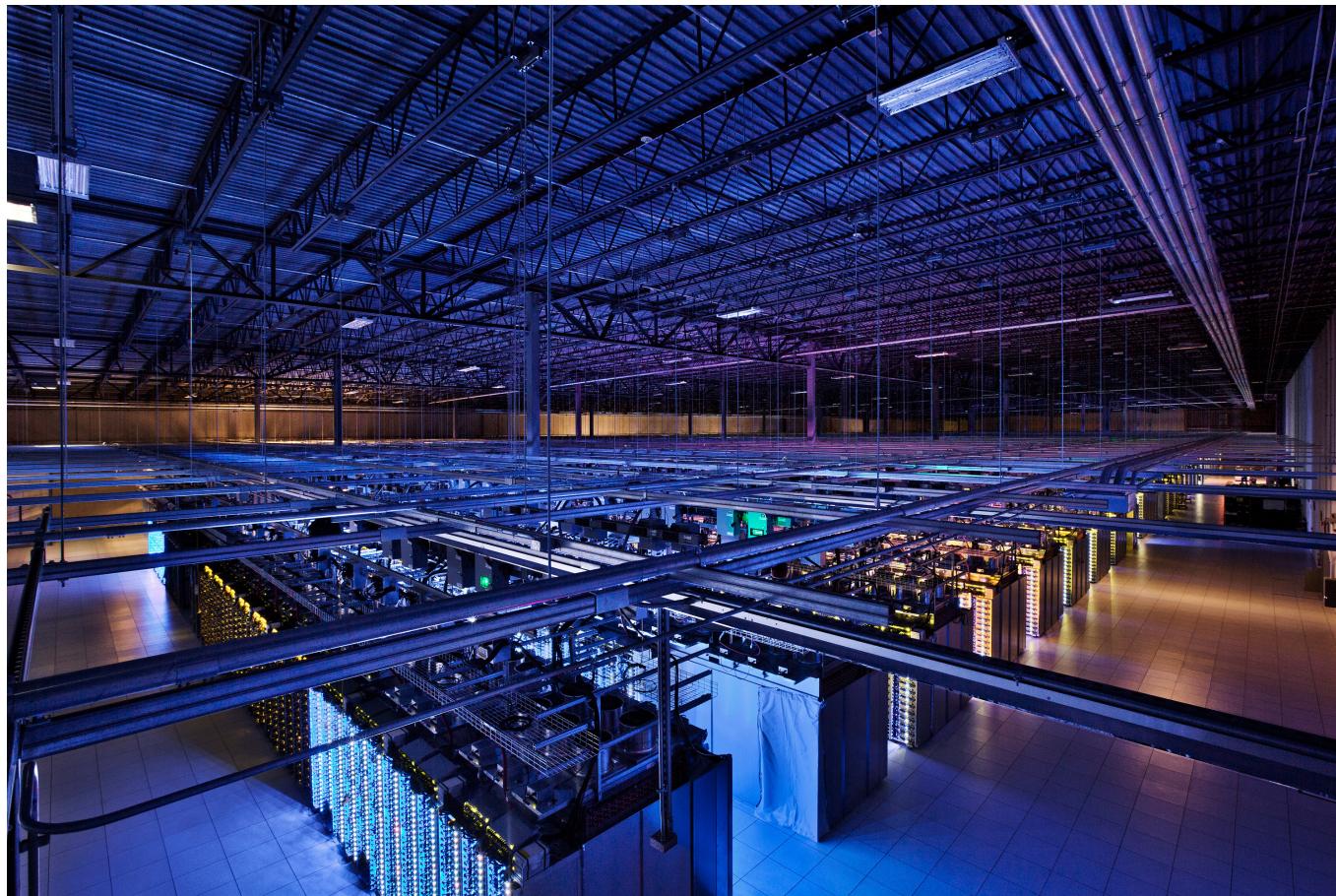


PKI (Public-Key Infrastructure)

تعريف ۱

یک چارچوب است متشکل از سخت افزارها، نرم افزارها، سیاست ها، استانداردها و دستورالعمل ها برای مدیریت کلید عمومی، مدیریت شناسه، تولید، توزیع، ذخیره سازی، ابطال و مدیریت گواهی نامه.

# مدیریت گواهینامه‌ها - موجودیت پایانی

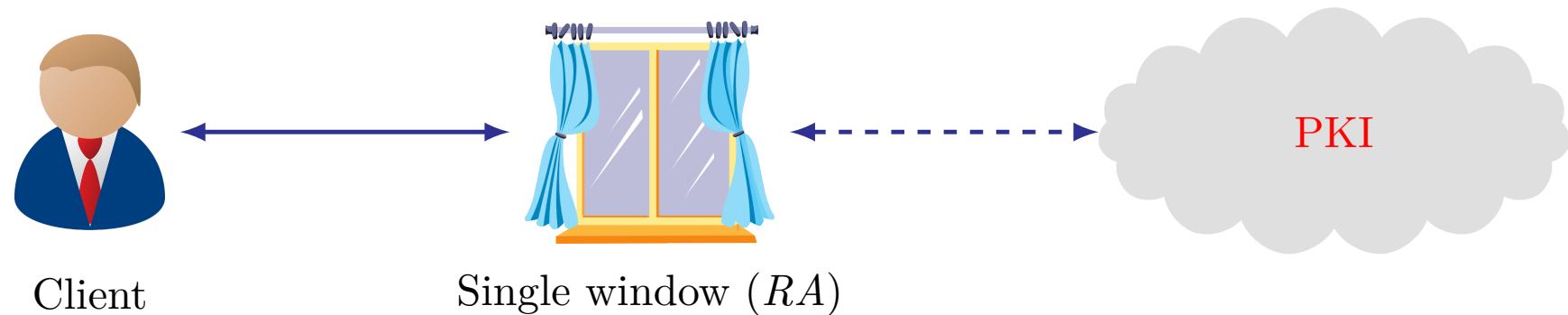


موجودیت پایانی (End Entity)

تعريف ۲

کاربران انسانی، ماشین و هر شی‌ای که بتواند از گواهینامه (Certificate) بهره ببرد.

# مدیریت گواهینامه‌ها - پنجره واحد



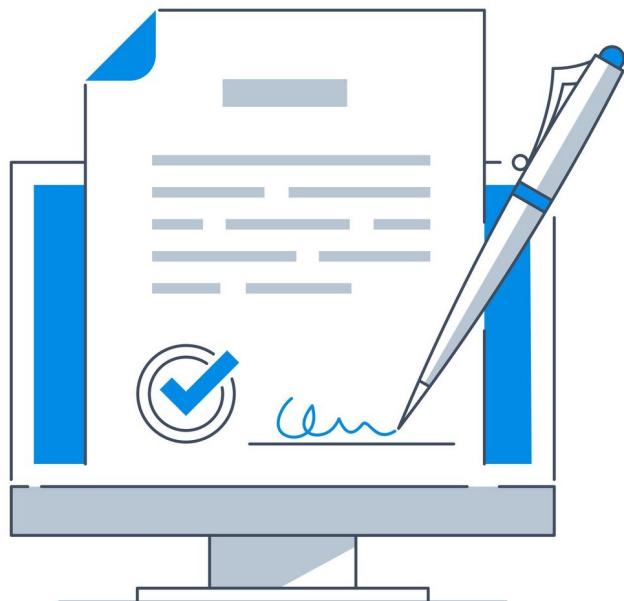
ثبت نام و تایید هویت کاربر و تخصیص شناسه به او توسط Registration

Front-end :RA (Registration Authority) یا به نوعی پنجره واحد برای دریافت درخواست‌ها و تایید

هویت کاربران

# مدیریت گواهینامه‌ها - تولید کلیدها

:CA (Certificate Authority) 



- تولید کلید عمومی و کلید محرمانه
- تولید گواهینامه برای کاربر به همراه امضای آن
- توزیع گواهینامه (Distributing)
- بروزرسانی گواهینامه (Update): زمان عمر کلید تمام شده.
- ابطال گواهینامه (Revoking) قبل از پایان عمر کلید.
- اگر کلیدمان گم شد؟ سازوکار Key Pair Recovery

## مدیریت گواهینامه‌ها - تاییدکننده

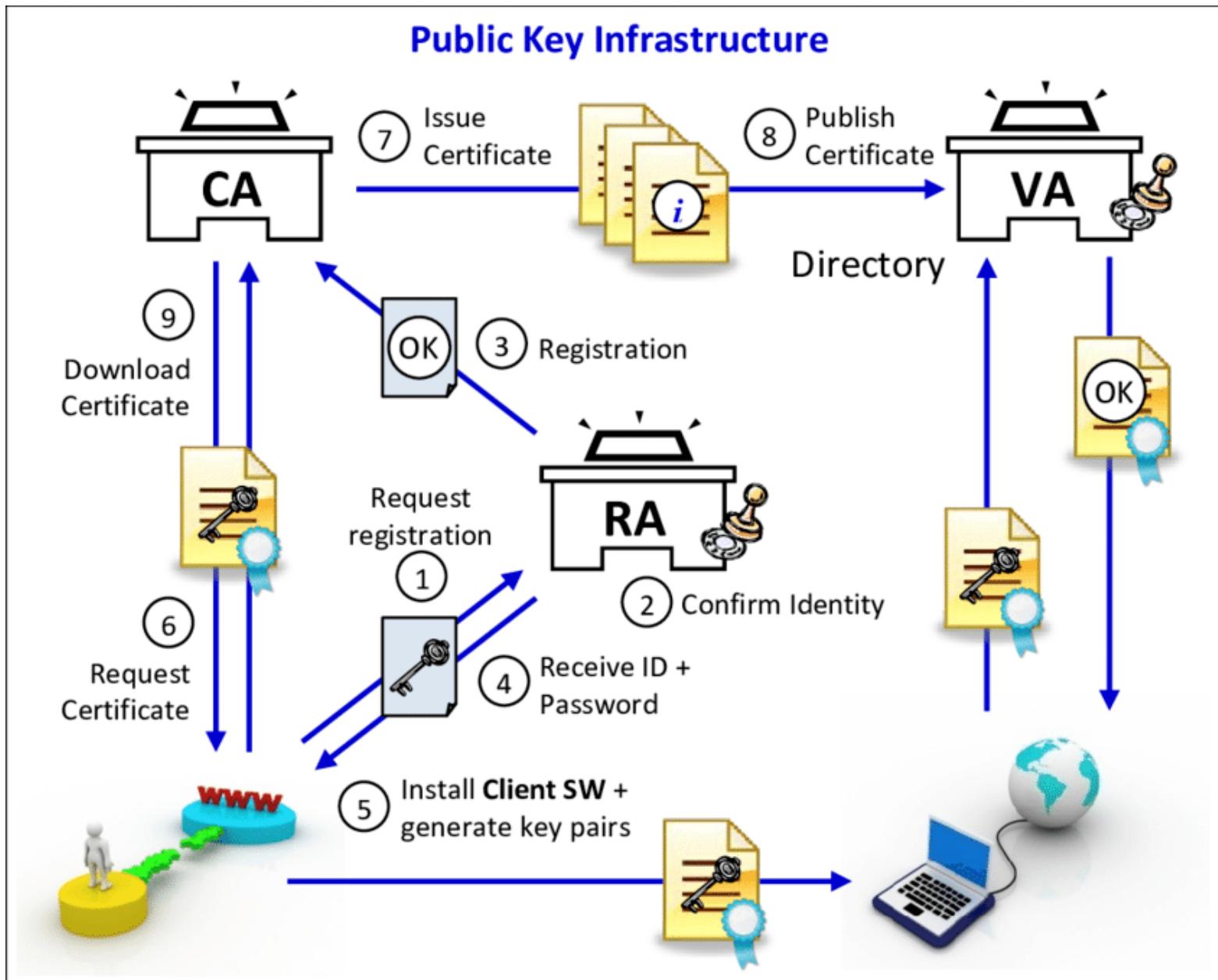


VA (Verification Authority)

تعريف ۳

مسئولیت اعتبارسنجی گواهینامه‌ها را برعهده دارد. در حقیقت، جایی است مورد اعتماد، که گواهینامه را تایید کند.

# نگاهی کلی به رویه PKI



مرجع گواهی نامه (CA) عموماً همه جنبه‌های مدیریت گواهی نامه برای یک PKI، شامل فازهای مدیریت چرخه حیات گواهی نامه را کنترل می‌کند. یک مرجع گواهی نامه، گواهی نامه‌هایی را صادر می‌کند که تأیید می‌کنند که موضوع چاپ شده روی گواهی نامه، مالک کلید عمومی است. در یک سیستم PKI، مشتری یک CA جفت کلید عمومی-خصوصی تولید می‌کند. کلید عمومی و اطلاعاتی که روی گواهی نامه چاپ می‌شوند، به فرستاده می‌شوند. سپس CA، یک گواهی نامه دیجیتال ایجاد می‌کند که شامل کلید عمومی کاربر و ویژگی‌های گواهی نامه است. گواهی نامه توسط CA امضا می‌شود که این امضا توسط کلید محرمانه مرجع ساخته می‌شود. وقتی که گواهی نامه به کاربر تحویل داده می‌شود، او می‌توانند گواهی امضا شده را ارائه کند و دریافت کننده می‌تواند اعتماد کند که این گواهی نامه متعلق به مشتری است زیرا با جفت کلید عمومی-خصوصی مطابقت دارد. یک CA، گواهی نامه‌هایی صادر می‌کند که شامل یک کلید عمومی و هویت صاحب آن است. کلید محرمانه مرتبط، صرفاً در اختیار صاحب آن است. زمانی که یک CA، یک گواهی نامه را تأیید می‌کند، به کاربران و شخصیت‌هایی که بر اساس این گواهی نامه کار می‌کنند این اطمینان را می‌دهد که بتوانند به اطلاعات منتقل

شده بر اساس گواهی مذکور اعتماد کنند.

CA مسئولیت این جمله را می‌پذیرد: «بله، این شخص همان کسی است که ادعا می‌کند و ما (یعنی CA) آن را تأیید می‌کنیم». سپس کاربری که با این گواهی نامه کار می‌کند، اگر درستی امضای دیجیتال مربوط به CA را تشخیص دهد، می‌تواند مطمئن باشد که کلید عمومی، حقیقتاً متعلق به همان هویتی است که گواهی برای آن صادر شده است.

رمزنگاری با کلید عمومی برای رمز کردن ارتباط دو طرفه به کار می‌رود. فرض کنید که یک کاربر در صفحه بانک خود با آدرس [www.bank.example](http://www.bank.example) وارد می‌شود تا خدمات بانکی برخط انجام دهد. هنگام باز کردن این صفحه، کاربر، یک کلید عمومی همراه با تمام اطلاعات صفحه دریافت می‌کند. زمانی که کاربر، اطلاعاتی را در صفحه بانک وارد و تأیید می‌کند، اطلاعات پیش از فرستاده شدن به وسیله مرورگر سایت و با استفاده از کلید عمومی ارائه شده توسط [www.bank.example](http://www.bank.example) رمزنگاری می‌شود. کلیدی که به وسیله آن اطلاعات را می‌توان رمزگشایی کرد، کلید محترمانه است که تنها در اختیار بانک است. در نتیجه، حتی اگر کسی بتواند به داده‌هایی که رد و بدل

شده دسترسی پیدا کند، نمی‌تواند آن را رمزگشایی کند، چون کلید محرمانه را در اختیار ندارد.

این مکانیزم تنها زمانی قابل اعتماد است که کاربر مطمئن باشد، کسی که با او در ارتباط است، بانک است. اگر کاربر آدرس [www.bank.example](http://www.bank.example) را وارد کند، ولی یک سایت تقلبی (که خود را به جای بانک جامی‌زند) اطلاعات صفحه بانک را به مرورگر بفرستد، همزمان با صفحه تقلبی یک کلید عمومی تقلبی نیز به کاربر می‌فرستد. کاربر فرم را با اطلاعات شخصی‌اش پر می‌کند و با تأیید آن، داده‌ها با کلید عمومی تقلبی، رمزنگاری می‌شود. صفحه تقلبی به اطلاعات کاربر دست می‌یابد، زیرا کلید محرمانه متناظرش را نیز در اختیار دارد.

مرجع صدور گواهی دیجیتال، یک سازمان است که کلیدهای عمومی، صاحبان آنها، و همه افراد مرتبط با اعتماد این سازمان را نگه داری می‌کند. زمانی که مرورگر، کلید عمومی را از [www.bank.example](http://www.bank.example) دریافت می‌کند، می‌تواند با CA ارتباط برقرار کند و استعلام بگیرد که آیا واقعاً کلید عمومی متعلق به [www.bank.example](http://www.bank.example) است یا خیر.

در عمل، این زنجیره‌ها تمایل دارند که با زنجیره‌های دیگر پیوند داشته باشند (اغلب از مراجع صدور گواهی‌نامه

دیگر)، و آن مراجع صدور گواهی نامه غالباً تصمیم می‌گیرند که به یکدیگر اعتماد کنند و گواهی نامه‌های امضا شده یکدیگر را که توسط CA دیگری امضا شده است، را بدون این که خودشان اعتبارسنجی کنند، بپذیرند. این امر را فدراسیون می‌نامند و در حالی که این امر، اوضاع را آسان‌تر می‌کند، اما به این معنی هم هست که فروشگاه اعتماد تنها در حد ضعیفترین پیوند، امنیت دارد. هر گواهی نامه می‌تواند توسط بیش از یک CA امضا شود که اعتماد پذیری آن را افزایش می‌دهد. زمانی که بیش از یک CA یک گواهی نامه را امضا می‌کند، آن را cross-signing می‌نامند. Root-CA، یک CA قابل اعتماد است که مجوز تأیید هویت یک شخص را دارد و نیز حق دارد که گواهی نامه ریشه‌ای را که به کاربر داده می‌شود را امضا کند. گواهینامه معتبر شناخته می‌شود؛ زیرا توسط Root-CA معتبری، تأیید و امضا شده است. گواهی نامه‌های SSL بر روی یک ساختار به نام زنجیره گواهی نامه عمل می‌کنند. منظور از زنجیره گواهی نامه، شبکه‌ای از گواهی نامه‌ها است که از شرکت صادرکننده گواهی نامه (یا همان مرجع صدور مجوز) آغاز می‌شود. این گواهی نامه‌ها شامل گواهی نامه‌های ریشه‌ای، گواهی نامه‌های میانی، و گواهی نامه‌های خدمت‌گزار (برگ) می‌باشند. گواهی نامه‌های SSL که مشتریان آنها را از جاهايی مثل

فروشگاه ComodoSSLStore خریداری می‌کند، در انتهای زنجیره گواهی نامه هستند. اما این زنجیره، به علاوه شامل گواهی نامه‌های واسط و ریشه‌ای نیز می‌باشد.

مرجع صدور گواهی نامه میانی (واسط) یک مرجع صدور گواهی نامه واسط، یک CA مورد اعتماد است و در زنجیره، بین Root-CA و گواهی نامه مشتری که کاربر آن را ثبت نام کرده است، مورد استفاده قرار می‌گیرد. از آن جا که CA Root، مرجع صدور واسط را امضا می‌کند و به آن اعتماد دارد، گواهی نامه‌هایی که از سوی مرجع گواهی نامه واسط ایجاد می‌شوند، قابل اعتمادند. PKI مربوط به SecureW2 همیشه از CA واسط برای تولید گواهی نامه‌های مشتری برای احراز اصالت Wi-Fi استفاده می‌کند، زیرا بهترین روش است. CA واسط مربوط به SecureW2 هیچ گاه در معرض خطر قرار نمی‌گیرد؛ زیرا برای CA واسط، یک سطح سخت‌افزاری از رمزنگاری برای کلید محربمانه مورد استفاده قرار می‌گیرد.

از نمونه این CA Public ها که همه به آنها در محیط اینترنت اعتماد دارند می‌توانیم به VeriSign و GeoTrust اشاره کنیم

مستقیماً به مرکز اصلی یا همان ستاد اصلی صادر کننده گواهینامه دیجیتال مراجعه کنید بلکه باید از مراکز زیردستی یا میانی برای دریافت این Certificate‌ها استفاده کنید.

# اولین میلی ثانیه‌ها در اینترنت

# اولین میلی ثانیه‌ها در اینترنت



☞ چه اتفاقی رخ می‌دهد که مرورگر ما می‌فهمد که به سایت معتبری وصل شدیم؟ چگونه امنیت این ارتباط

تامین می‌شود؟

☞ ما باید بر طبق استاندارد عمل کنیم:

SSL 2.0 (1995), SSL 3.0 (1996), TLS 1.0 (1999), TLS 1.1 (2006), TLS 1.2 (2008), TLS 1.3 (2018)

HTTPs و TLS (Transport Layer Security) ، SSL (Secure Sockets Layer) تفاوت



## اولین میلی ثانیه‌ها در اینترنت (ادامه)

1...	10.1...	192.168.88.249	94.182.146.59	TCP	76 37280 → 443 [SYN] Se
1...	10.1...	94.182.146.59	192.168.88.249	TCP	76 443 → 37280 [SYN, AC
1...	10.1...	192.168.88.249	94.182.146.59	TCP	68 37280 → 443 [ACK] Se
1...	10.1...	192.168.88.249	94.182.146.59	TLSv1.2	585 Client Hello
1...	10.2...	94.182.146.59	192.168.88.249	TLSv1.2	1316 Server Hello

Frame 1222: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface a  
Linux cooked capture v1

Internet Protocol Version 4, Src: 192.168.88.249, Dst: 94.182.146.59

Transmission Control Protocol, Src Port: 37280, Dst Port: 443, Seq: 0, Len: 0

Source Port: 37280

Destination Port: 443

[Stream index: 20]

[Conversation completeness: Incomplete, DATA (15)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 2927472039

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 0

Acknowledgment number (raw): 0

وقتی شما عبارت <https://www.amazon.com> را تایپ می‌کنید، مرورگر می‌فهمد که باید به شماره درگاه

443 خدمت‌گزار درخواست دهد.

ابتدا فرایند دست‌یابی به آدرس IP با استفاده از خدمت‌گزار DNS صورت می‌پذیرد.

# اولین میلی ثانیه‌ها در اینترنت (ادامه)

1...	10.1...	192.168.88.249	94.182.146.59	TLSv1.2	585	Client Hello
1...	10.2...	94.182.146.59	192.168.88.249	TLSv1.2	1316	Server Hello

## Transport Layer Security

```
‐ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 512
‐ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    Version: TLS 1.2 (0x0303)
‐ Random: 3990da6c82416ea97337ab634106f140538e05e6a02d0c344d487dbdd918faa2
    Session ID Length: 32
    Session ID: d269b0d6c1ef4d7884105389ab77183385ccf2649bf6f81754a08641c23c8db9
    Cipher Suites Length: 32
‐ Cipher Suites (16 suites)
    Compression Methods Length: 1
‐ Compression Methods (1 method)
    Extensions Length: 403
```

اولین پیامی که توسط مشتری ارسال می‌شود، پیامی است به نام Client hello

- مهر زمانی از January 1, 1970 به همراه یک مقدار تصادفی
- مرورگر چه الگوریتم‌هایی را برای رمزگذاری، فشرده‌سازی و امضای دیجیتال می‌تواند پشتیبانی کند؟

# اولین میلی ثانیه‌ها در اینترنت (ادامه)

1...	10.1...	192.168.88.249	94.182.146.59	TLSv1.2	585 Client Hello
1...	10.2...	94.182.146.59	192.168.88.249	TLSv1.2	1316 Server Hello

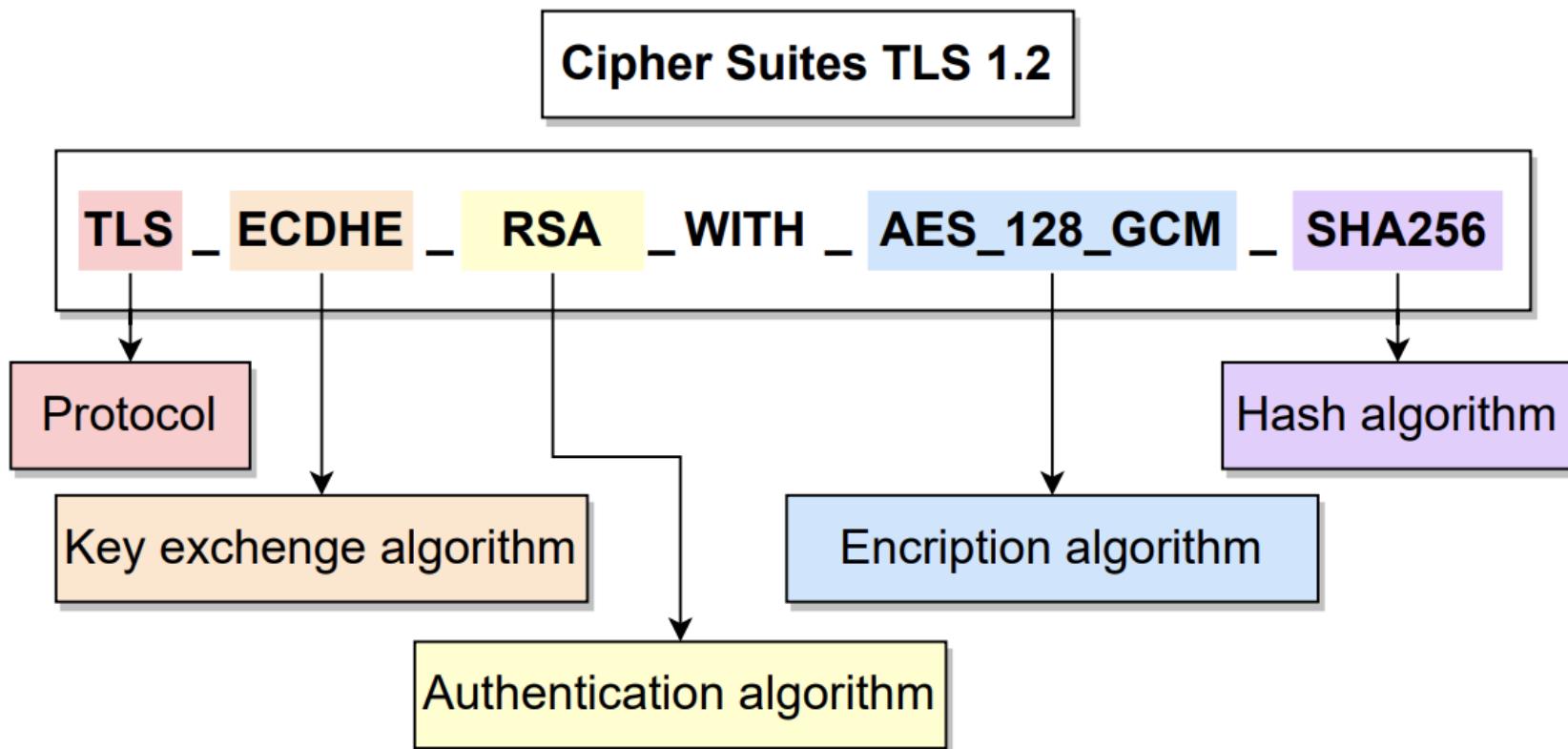
## Transport Layer Security

```
- TLSv1.2 Record Layer: Handshake Protocol: Server Hello
  Content Type: Handshake (22)
  Version: TLS 1.2 (0x0303)
  Length: 93
- Handshake Protocol: Server Hello
  Handshake Type: Server Hello (2)
  Length: 89
  Version: TLS 1.2 (0x0303)
  ▶ Random: 638add233039f428bc4b77377c7e3aa2d0718b3c3bcc522d61dc3dbf5b2ec248
  Session ID Length: 32
  Session ID: 4298c81df98006ceee723b50698dd521bd6836f0dda10179371e69dc1390c099
  Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
  Compression Method: null (0)
  Extensions Length: 17
- Extension: server_name (len=0)
  Type: server_name (0)
```

با رسیدن پیام Server Hello، می‌توان دریافت که خدمت‌گزار درخواست ما را پذیرفته است.

- مهر زمانی، و تخصیص شناسه‌ای برای جلسه
- انتخاب الگوریتم امنیتی: پیشنهاد مشتری و انتخاب خدمت‌گزار

# اولین میلی ثانیه‌ها در اینترنت (ادامه)



# اولین میلی ثانیه‌ها در اینترنت (ادامه)

1... 10.2... 94.182.146.59 192.168.88.249 TLSv1.2 1132 Certificate, Server Key Exchan

Transport Layer Security

- TLSv1.2 Record Layer: Handshake Protocol: Certificate
  - Content Type: Handshake (22)
  - Version: TLS 1.2 (0x0303)
  - Length: 4102
- Handshake Protocol: Certificate
  - Handshake Type: Certificate (11)
  - Length: 4098
  - Certificates Length: 4095
  - Certificates (4095 bytes)
    - Certificate Length: 1893
    - Certificate: 3082076130820649a003020102021024d49af42aedcea23b57c90ead
      - signedCertificate
        - version: v3 (2)
        - serialNumber: 0x24d49af42aedcea23b57c90eaddc5e0f
      - signature (sha256WithRSAEncryption)
      - issuer: rdnSequence (0)
        - rdnSequence: 4 items (id-at-commonName=Certum Domain Validation)
          - RDNSequence item: 1 item (id-at-countryName=PL)
          - RDNSequence item: 1 item (id-at-organizationName=Unizeto Tec
          - RDNSequence item: 1 item (id-at-organizationalUnitName=Certu
          - RDNSequence item: 1 item (id-at-commonName=Certum Domain Val
      - validity

## Certificate Viewer: \*.tabnak.ir

General Details

### Issued To

Common Name (CN)	*.tabnak.ir
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

### Issued By

Common Name (CN)	Certum Domain Validation CA SHA2
Organization (O)	Unizeto Technologies S.A.
Organizational Unit (OU)	Certum Certification Authority

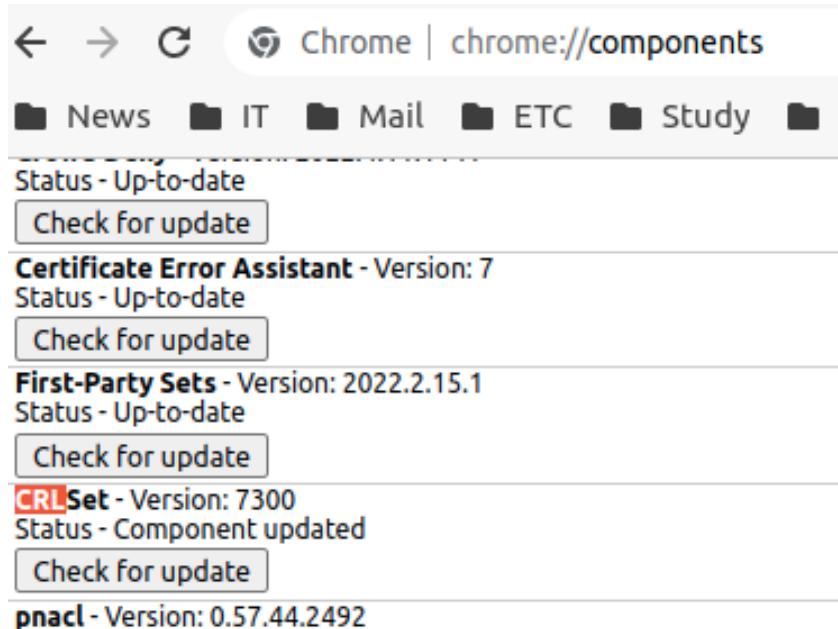
### Validity Period

Issued On	Monday, July 18, 2022 at 9:52:17 AM
Expires On	Tuesday, July 18, 2023 at 8:52:16 AM

### Fingerprints

SHA-256 Fingerprint	A0 8E E4 CE E4 29 6D 4D AF 03 0B 0F B8 53 A1 FC FD 77 3B 98 89 81 B4 25 9C FB B8 38 0B 08 91 9D
SHA-1 Fingerprint	F7 82 25 28 51 80 FE 40 C1 5F 0B 23 C5 FD 9E 8A 9E F3 CE 58

# اولین میلی ثانیه‌ها در اینترنت (ادامه)



برای مدیریت ابطال گواهینامه‌ها دو روند کلی وجود دارد:

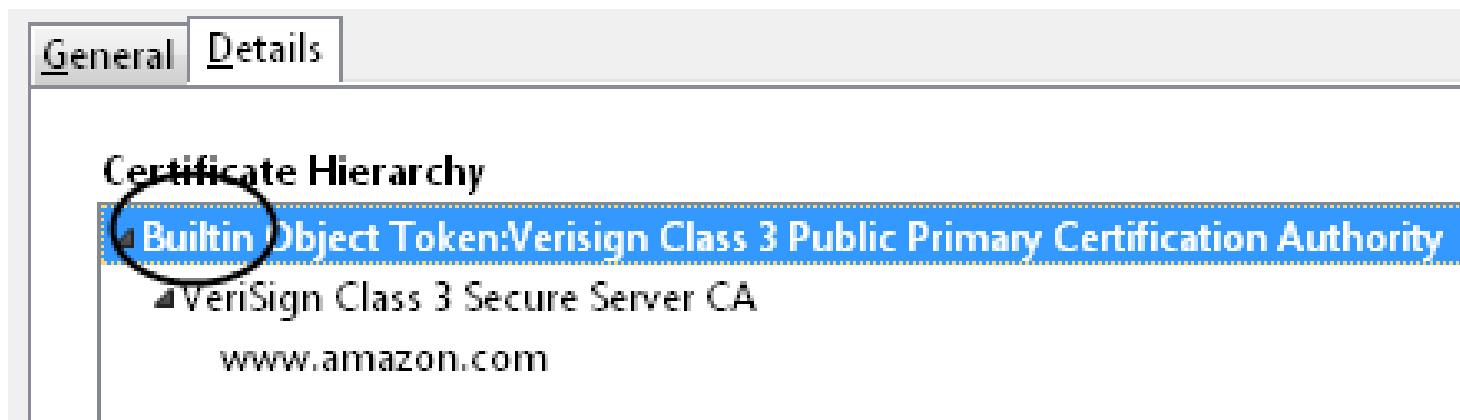
Chrome: لیستی هست که به صورت دوره‌ای بروز می‌شود. مانند CRL (Certificate Revocation List) •

Firefox: به صورت برخط استعلام می‌شود. مانند OCSP (Online Certificate Status Protocol) •

در روش CRL، شماره سریال گواهینامه‌های باطله را به صورت دوره‌ای به اطلاع همگان می‌رساند. سادگی و عدم نیاز به داشتن یک مرکز از فواید این روش است. اما مجموعه فهرست گواهینامه‌های باطله دارای حجم نسبتاً بالایی است در این صورت برای دانلود و ذخیره‌سازی ایجاد اشکال می‌کند، و همچنین تازمان اطلاع‌رسانی ممکن است دشمن سوءاستفاده بکند.

در روش OCSP، و با توجه به مشکل دو روش قبلی برای جبران نیاز به یک خدمات است که تحت شبکه اینترنت وظیفه اطلاع‌رسانی را از طریق سیستم پرسش و پاسخ انجام دهد. این خدمات از طریق پروتکل HTTP صورت می‌گیرد. در این روش امکان پردازش و ذخیره‌سازی در طرف کاربر برداشته شده است و سیستم مبتنی بر پرسش و پاسخ است. روش OCSP از این ویژگی برخوردار است که یک زنجیره توزیع شده قابل اعتماد را در سطح شبکه تشکیل داده و برای افزایش اطمینان سرعت پاسخ‌گویی، بار پاسخ پرسش‌ها را بین یکدیگر توزیع کرده و اجازه ندهد یکی از آنها زیر بار زیاد در هم شکند.

# اولین میلی ثانیه‌ها در اینترنت (ادامه)



- ما می‌توانیم سلسله مراتبی از امضاها داشته باشیم.
- امضای بسیاری از CA‌های معتبر به مانند VeriSign Class 3 Public Primary Certification Authority در خود مرورگرها وجود دارد.

- ۱ در ۱۵ شهریور ۱۳۹۰ گزارشی مبنی بر جعل ۵۳۱ گواهینامه شرکت Diginotar منتشر شد. 
- ۲ نبود ولی در حال تبدیل شدن به Root CA بود، ولی در سال ۲۰۱۱ اعلام ورشکستگی کرد. 
- ۳ در حقیقت هکرها توانسته بودند به سیستم تولید گواهینامه این شرکت نفوذ کنند و این گواهی‌های جعلی را ایجاد کنند. 
- ۴ صدور گواهینامه‌های جعلی توسط فرد یا نهادهایی از ایران ادامه می‌یابد، آثار آخرین گواهینامه احتمالی، صادر شده به تاریخ ۲۰ ژوئیه یا ۲۹ تیر ماه برمی‌گردد. 
- ۵ اولین گواهی‌نامه‌های جعل شده برای Google بود، و تقریباً کل استفاده نیز در ایران صورت پذیرفته بود. 

# اولین میلی ثانیه‌ها در اینترنت (ادامه)

1...	10.18910...	192.168.88.249	94.182.146.59	TLSv1.2	585 Client Hello
1...	10.21347...	94.182.146.59	192.168.88.249	TLSv1.2	1316 Server Hello
1...	10.21397...	94.182.146.59	192.168.88.249	TLSv1.2	1132 Certificate, Server Key Exchange, Server Hello Done
1...	10.21659...	192.168.88.249	94.182.146.59	TLSv1.2	194 Client Key Exchange, Change Cipher Spec, Encrypted

Frame 1230: 1132 bytes on wire (9056 bits), 1132 bytes captured (9056 bits) on interface any, id 0  
Linux cooked capture v1  
Internet Protocol Version 4, Src: 94.182.146.59, Dst: 192.168.88.249  
Transmission Control Protocol, Src Port: 443, Dst Port: 37280, Seq: 3745, Ack: 518, Len: 1064  
[3 Reassembled TCP Segments (4107 bytes): #1226(1150), #1228(2496), #1230(461)]  
Transport Layer Security  
  ↳ TLSv1.2 Record Layer: Handshake Protocol: Certificate  
Transport Layer Security  
  ↳ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange  
    Content Type: Handshake (22)  
    Version: TLS 1.2 (0x0303)  
    Length: 589  
  ↳ Handshake Protocol: Server Key Exchange  
    Handshake Type: Server Key Exchange (12)  
    Length: 585  
  ↳ EC Diffie-Hellman Server Params  
    Curve Type: named\_curve (0x03)  
    Named Curve: secp256r1 (0x0017)  
    Pubkey Length: 65  
    Pubkey: 045616fb2eacc3cda0b66a48b4415f0d26addc446368908286e6c87228c2977ac4c98efa...  
  ↳ Signature Algorithm: rsa\_pkcs1\_sha256 (0x0401)  
    Signature Hash Algorithm Hash: SHA256 (4)  
    Signature Hash Algorithm Signature: RSA (1)  
    Signature Length: 512  
    Signature: 67364bb557edfde067e6783847d899934c0782a60782078cb592f2928df6113049a64179...  
  ↳ TLSv1.2 Record Layer: Handshake Protocol: Server Hello Done  
    Content Type: Handshake (22)  
    Version: TLS 1.2 (0x0303)  
    Length: 4  
  ↳ Handshake Protocol: Server Hello Done  
    Handshake Type: Server Hello Done (14)  
    Length: 0

خدمت‌گزار پیامی را بروتکل ECDH برای مشتری ارسال می‌کند.

# اولین میلی ثانیه‌ها در اینترنت (ادامه)

1...	10.21659...	192.168.88.249	94.182.146.59	TLSv1.2	194 Client Key Exchange, E
1...	10.22022...	94.182.146.59	192.168.88.249	TLSv1.2	119 Change Cipher Spec, E
1...	10.22038...	192.168.88.249	94.182.146.59	TLSv1.2	729 Application Data

  
Frame 1232: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits) on interface ar					
Linux cooked capture v1					
Internet Protocol Version 4, Src: 192.168.88.249, Dst: 94.182.146.59					
Transmission Control Protocol, Src Port: 37280, Dst Port: 443, Seq: 518, Ack: 4809, Len:					
Transport Layer Security					
▼ TLSv1.2 Record Layer: Handshake Protocol: Client Key Exchange					
Content Type: Handshake (22)					
Version: TLS 1.2 (0x0303)					
Length: 70					
▼ Handshake Protocol: Client Key Exchange					
Handshake Type: Client Key Exchange (16)					
Length: 66					
▼ EC Diffie-Hellman Client Params					
Pubkey Length: 65					
Pubkey: 04b392c59a79539115d4c648e7ebcfaf770794efc45de7e407b7625ee37c77e323147ebb1					
▶ TLSv1.2 Record Layer: Change Cipher Spec Protocol: Change Cipher Spec					
▶ TLSv1.2 Record Layer: Handshake Protocol: Encrypted Handshake Message					

مشتری پیامی را بطبق پروتکل ECDH برای خدمت‌گزار ارسال می‌کند.

در نخستین گام وقتی شما سایتی به مانند <https://tabnak.ir> را می‌زنید، مرورگر شما با استفاده از پروتکل DNS به دنبال IP آن می‌گردد. پس از پیدا شدن آدرس IP، سیستم عامل شما یک ارتباط TCP با خدمت‌گزار ایجاد می‌کند. این ارتباط به دلیل HTTPS بودن سایت، در شماره درگاه 443 خدمت‌گزار ایجاد می‌شود.

اولین پیام TLS که ما آن را با نام Client hello می‌شناسیم، از سمت مشتری به خدمت‌گزار ارسال می‌شود. در این پیام نسخه پروتکل TLS، یک عدد تصادفی و یک شناسه برای نشست ارتباطی به همراه قابلیت‌های امنیتی مشتری، برای خدمت‌گزار ارسال می‌شود. خدمت‌گزار با رسیدن این پیام، یک پیام به نام Server hello برای مشتری ارسال می‌کند. این پیام نیز شامل همان موارد و همچنین انتخاب خدمت‌گزار از بین قابلیت‌های امنیتی مشتری است که در پیام قبلی برای او ارسال کرده بود.

در مرحله بعدی، خدمت‌گزار گواهینامه را برای مشتری ارسال می‌کند. مشتری باید موارد زیر را چک کند:

- امضای دیجیتال گواهینامه: ممکن است سلسله مراتبی از امضاها داشته باشیم. معمولاً امضای CA‌های معروف در خود مرورگرها وجود دارد.

- زمان انقضا گواهینامه
  - چک کردن Hostname
  - آیا گواهینامه معتبر است؟ ممکن است ابطال شده باشد!
- در ادامه زیر پروتکل ECDH (Elliptic Curve Diffie Hellman) به منظور اجرای رویه تبادل کلید اجرا می‌گردد.



- ☞ می خواهیم یک راز را بین  $n$  نفر به اشتراک بگذاریم به گونه ای که راز تنها در صورتی آشکار شود که حداقل  $t$  نفر از این  $n$  نفر با یکدیگر مشارکت کنند.
- ☞ هیچ کس به تنها بی نباید اطلاعاتی راجع به راز داشته باشد.
- ☞ ایده شامیر: یافتن یک منحنی درجه  $1 - t$  با استفاده از  $t$  نقطه.

## مطالب پست‌فرم - گواہینا مہ

X.509

روند استاندارد X.509 از July, 1988 آغاز شد. این ساختار برای یک سیستم سلسه مراتبی به منظور ایجاد شکل متحد و یکنواخت جهانی برای گواهی نامه دیجیتال تصویب و معرفی شد، که امروزه با ویژگی های فراوان و چشمگیری در دسترس عموم است.

ساختار X.509 به گونه ای است که مرکز صدور گواهینامه باید برای یک شخص حقیقی / حقوقی، آدرس پست الکترونیکی، آدرس DNS و یا اشیا با ساختار استاندارد گواهی نامه ای صادر کند. نیاز است یک ساختار استاندارد ویکپارچه برای X.509 وجود داشته باشد بر همین اساس IETF اصلاحات مد نظر خود را انجام داده است و تحت نسخه سوم صادر کرده است که با نام IETF PKIX Certificate شناخته می شود. عناصر موجود در گواهینامه X.509 به شرح زیر است:

**Version**: این فیلد در حقیقت بیانگر شماره نسخه گواهینامه است.

**Serial Number**: شماره سریال گواهینامه صادره توسط یک مرکز مشخص صدور گواهینامه (CA) است. در واقع مراکز صدور گواهینامه با این شماره به صورت منحصر به فرد کاربر را به همراه اطلاعاتش مشخص می کند.

SHA-256 With: این فیلد بیانگر الگوریتم به کار رفته در تولید گواهینامه است. برای مثال Algorithm ID بیان می‌کند که در این گواهینامه از توابع چکیده‌ساز SHA-256 و سیستم رمزنگاری RSA Encrypt استفاده شده است.

Validity: این فیلد تعیین کننده بازه‌ی تاریخ شروع و انقضا گواهینامه را بیان می‌کند.  
Subject: این فیلد بیان کننده نام حقیقی / حقوقی یک موجودیت است که کلید عمومی او در این گواهینامه تایید شده است. منظور از موجودیت: هر شخص، موسسه، آدرس EMail، و ... می‌باشد.

Subject Public Key Info: این فیلد دارای دو بخش است و هر آنچه را که در مورد کلید عمومی صاحب گواهینامه لازم است دیگران بدانند، در آن بیان شده است.

Public Key Algorithm: در این فیلد مقدار کلید عمومی کاربر قرار دارد. برای مثال اگر از ساختار RSA استفاده شود در این فیلد درای یک جفت مقدار  $(n, e)$  است. که مقدار  $n$  به عنوان پیمانه محاسبات بر مبانی ۱۶ در نظر گرفته می‌شود و هر بایت با علامت : از یکدیگر جدا می‌شوند. مقدار  $e$  به عنوان کلید عمومی بر مبنای

۱۰ می باشد.

Subject Public Key: در این فیلد شناسه الگوریتم رمزنگاری کلید عمومی صاحب گواهینامه بیان می گردد. معمولاً پرکاربردترین الگوریتم RSA با شناسه rsaEncryption است.

Issuer Unique Identifier (optional): شناسه جهانی و یکتا مرکز صدور گواهینامه را تعیین می کند. فعلاً تنظیم این فیلد اختیاری است.

Subject Unique Identifier (optional): شناسه جهانی و یکتا برای موجودیت صاحب گواهینامه است. فعلاً تنظیم این فیلد اختیاری است.

Extensions (optional): به کمک این فیلد می توان هر تعداد دلخواه مشخصات اضافی به گواهینامه افزود. Certificate Signature Algorithm در این فیلد الگوریتم به کار رفته شده برای امضای کل گواهینامه مشخص می شود. برای مثال md5WithRSAEncryption بیان می کند که از توابع چکیده ساز md5 به همراه سیستم رمزنگاری RSA در این امضا استفاده شده است.

در این فیلد کل فیلدهای قبلی گواهینامه توسط الگوریتم نام برده شده در فیلد قبلی Certificate Signature به وسیله یک توابع چکیده‌ساز و کلید خصوصی مرکز صدور گواهینامه امضا می‌شود. در واقع با وجود این فیلد امنیت گواهینامه به مرکز صدور وابسته می‌شود و از این طریق می‌توان مبحث بررسی زنجیره‌ای سلسله مراتب صدور گواهینامه را بیان کرد.

## مراجع

# فهرست اختصارات

## C

CA ..... Certificate Authority

CRL ..... Certificate Revocation List

## D

DNS ..... Domain Name System

E

ECDH ..... Elliptic Curve Diffie Hellman

I

IETF ..... Internet Engineering Task Force

IP ..... Internet Protocol

O

OCSP ..... Online Certificate Status Protocol

## P

PGP ..... Pretty Good Privacy

PKI ..... Public-Key Infrastructure

## R

RA ..... Registration Authority

## S

SSL ..... Secure Sockets Layer

## T

TCP ..... Transmission Control Protocol

TLS ..... Transport Layer Security

## V

VA ..... Verification Authority

## W

Wi-Fi ..... Wireless Fidelity

# واژه‌نامه انگلیسی به فارسی

C

Certificate ..... گواهینامه ..... Authentication ..... احراز اصالت .....

Certificate Life Cycle ..... چرخه حیات گواهی نامه ..... Attacker ..... حمله‌گر .....

Client ..... مشتری .....

Compression ..... فشرده‌سازی ..... B

A

Browser ..... مرورگر .....

## F D

امضای دیجیتال ..... چارچوب ..... Framework ..... Digital Signature .....

## H E

زمان انقضا ..... تابع چکیدهساز ..... Hash Function ..... Expiration Time .....

رمزنگاری ..... Encryption ..... موجودیت پایانی ..... End Entity .....

شناسه ..... Identity .....

میانی ..... Intermediate .....

Operating System ..... سیستم عامل .....

K

P تبادل کلید .. Key Exchange .....

Public Key ..... کلید عمومی .....

Port Number ..... شماره درگاه M

Private Key ..... کلید محرمانه ..... مردمیانی ..... Man in the middle .....

R O

Revocation ..... ابطال ..... برخط ..... Online .....

U

User ..... کاربر Server ..... خدمتگزار

Session ..... نشست

V

Validation ..... اعتبارسنجی T

Timestamp ..... مهر زمانی

Trust ..... اعتماد

Trusted ..... قابل اطمینان

# واژه‌نامه فارسی به انگلیسی

## ب

Online .....	برخط	Revocation ..... ابطال ..
		احراز اصالت .. Authentication ..
		اعتبارسنجی .. Validation ..
		اعتماد .. Trust ..
Hash Function .....	تابع چکیده‌ساز ..	Digital Signature .. امضای دیجیتال ..
Key Exchange .....	تبادل کلید ..	

ج

ر

Encryption .....	رمزگذاری .....	Framework .....	چارچوب .....
		Certificate Life Cycle .....	چرخه حیات گواهی نامه .....

ز

Expiration Time .....	زمان انقضا .....	ح
	Attacker .....	حمله‌گر .....

س

Operating System .....	سیستم عامل .....	خ
	Server .....	خدمت‌گزار .....

ش

User ..... کاربر Port Number ..... شماره درگاه

Public Key ..... کلید عمومی Identity ..... شناسه

Private Key ..... کلید محرمانه

ف

فشرده‌سازی ..... گ Compression .....

Certificate ..... گواهینامه

ق

قابل اطمینان ..... Trusted

م

مردمیانی ..... Man in the middle .....

مرورگر ..... Browser .....

مشتری ..... Client .....

موجودیت پایانی ..... End Entity .....

مهر زمانی ..... Timestamp .....

میانی ..... Intermediate .....

ن

نشست ..... Session .....