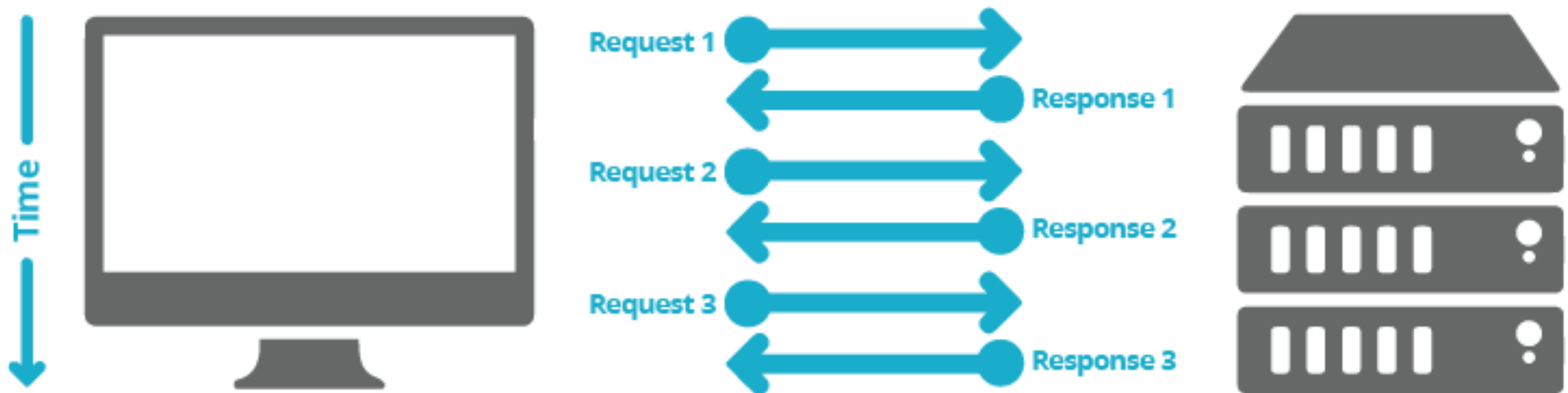


SSL / TLS



HTTP

SSL / TLS implementasyonuna neden ihtiyaç duyuldu ?



SSL / TLS Nedir ?

- SSL / TLS : İstemci ve sunucu arasındaki trafiğin şifreleyerek güvenli bir iletişim ortamı sağlayan protokoldür.
- HTTPS, HTTP protokolü üzerinde SSL/TLS çalıştırılmış halidir.
- Ayrıca gelen mesajın gerçekten göndericiden geldiğini doğrular.
- 443 portu kullanır.

Request URL: https://github.com/

Request method: GET

Remote address: 192.30.253.113:443

Status code: ● 200 OK ⓘ [Edit and Resend](#)

Version: HTTP/1.1

Website Identity

Website: **github.com**

Owner: **GitHub, Inc.**

Verified by: **DigiCert Inc**

Expires on: **May 17, 2018**

[View Certificate](#)

Privacy & History

Have I visited this website prior to today? **Yes, 1,905 times**

Is this website storing information (cookies) on my computer? **Yes**

[View Cookies](#)

Have I saved any passwords for this website? **Yes**

[View Saved Passwords](#)

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

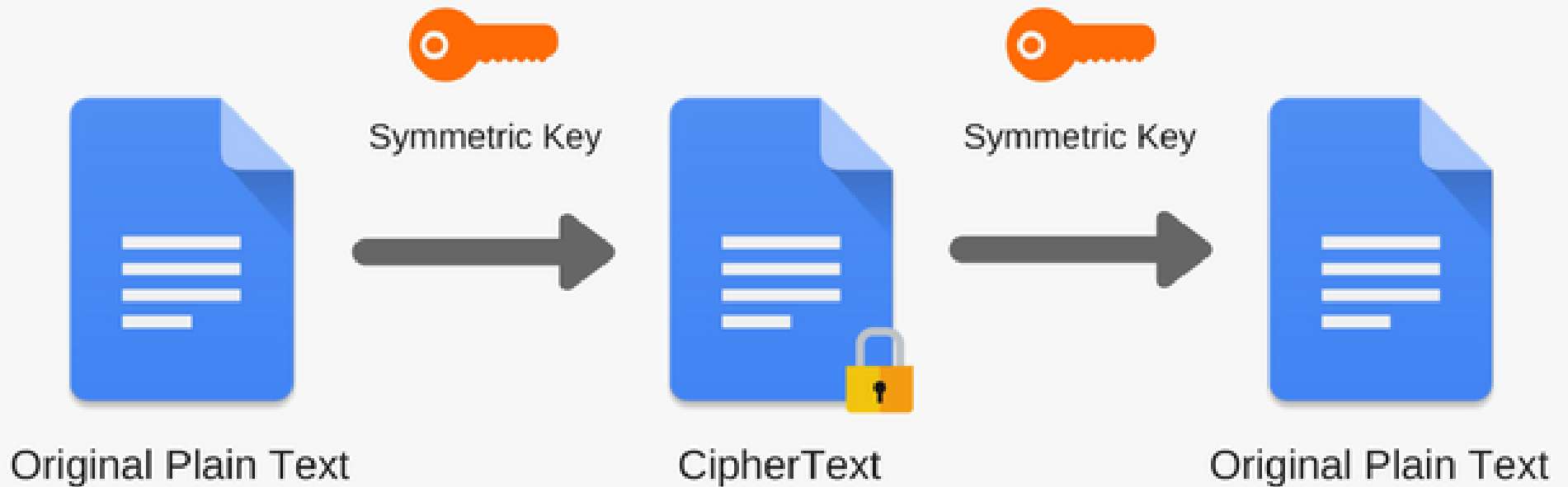
The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

[Help](#)

Simetrik Şifreleme

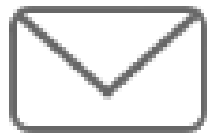
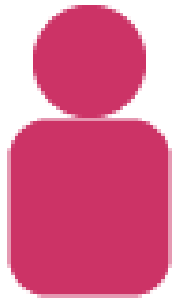
- Şifreleme için tek bir anahtar kullanılır.
- Gizli anahtar karşı taraf ile paylaşılacak zorundadır.
- Asimetrik şifrelemeye göre çok hızlıdır.
- Bazı örnek asimetrik algoritmalar; DES, AES, 3DES



Asimetrik Şifreleme

- İki farklı anahtar vardır; Public ve Private key
- Veriyi şifreleyen public anahtardır, çözen private anahtardır.
- Anahtar paylaşımına gerek yoktur.

Alice



+

**Bob's
public key**



-->



/

**Bob's
private key**



-->

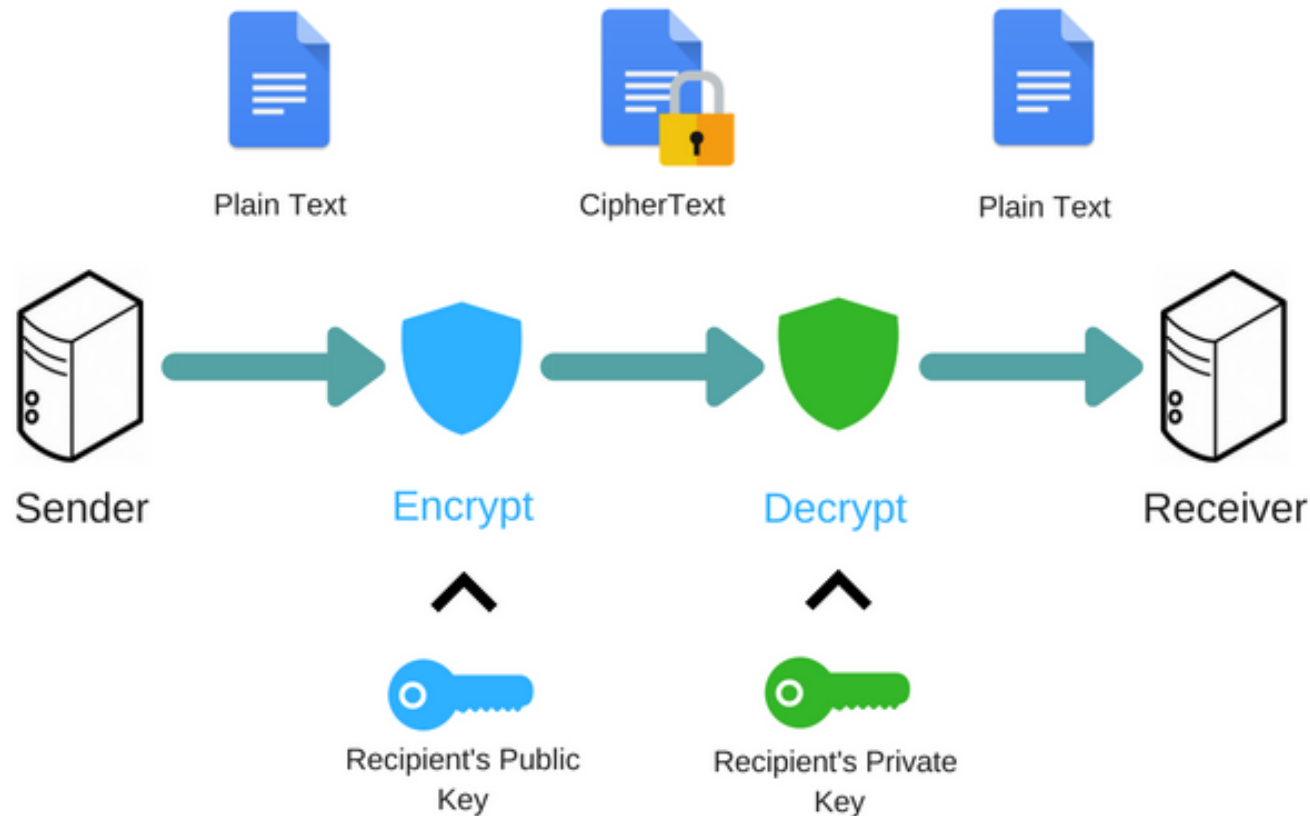


Bob



Asimetrik Şifreleme

- Anahtar paylaşımına gerek yoktur bu yüzden güvenli olma durumu yüksektir.
- Simetrik şifreleme algoritmalarına göre çok yavaştır.



Different keys are used to encrypt and decrypt the message

Diffie Helman - DF

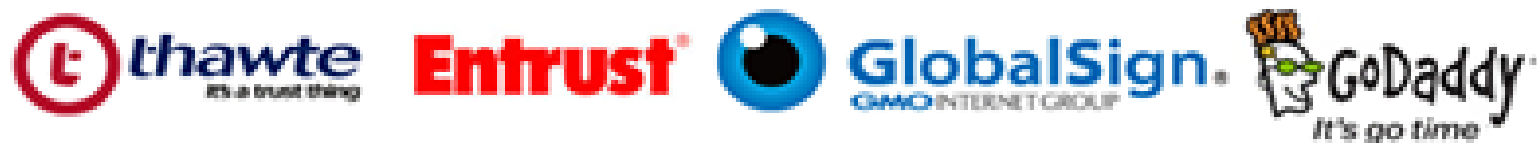
- Bir anahtar değişim algoritmasıdır.
- Tarafların güvensiz bir ortamda güvenli bir şekilde ortak bir anahtar üzerinde karar kılmalarını sağlar.

RSA

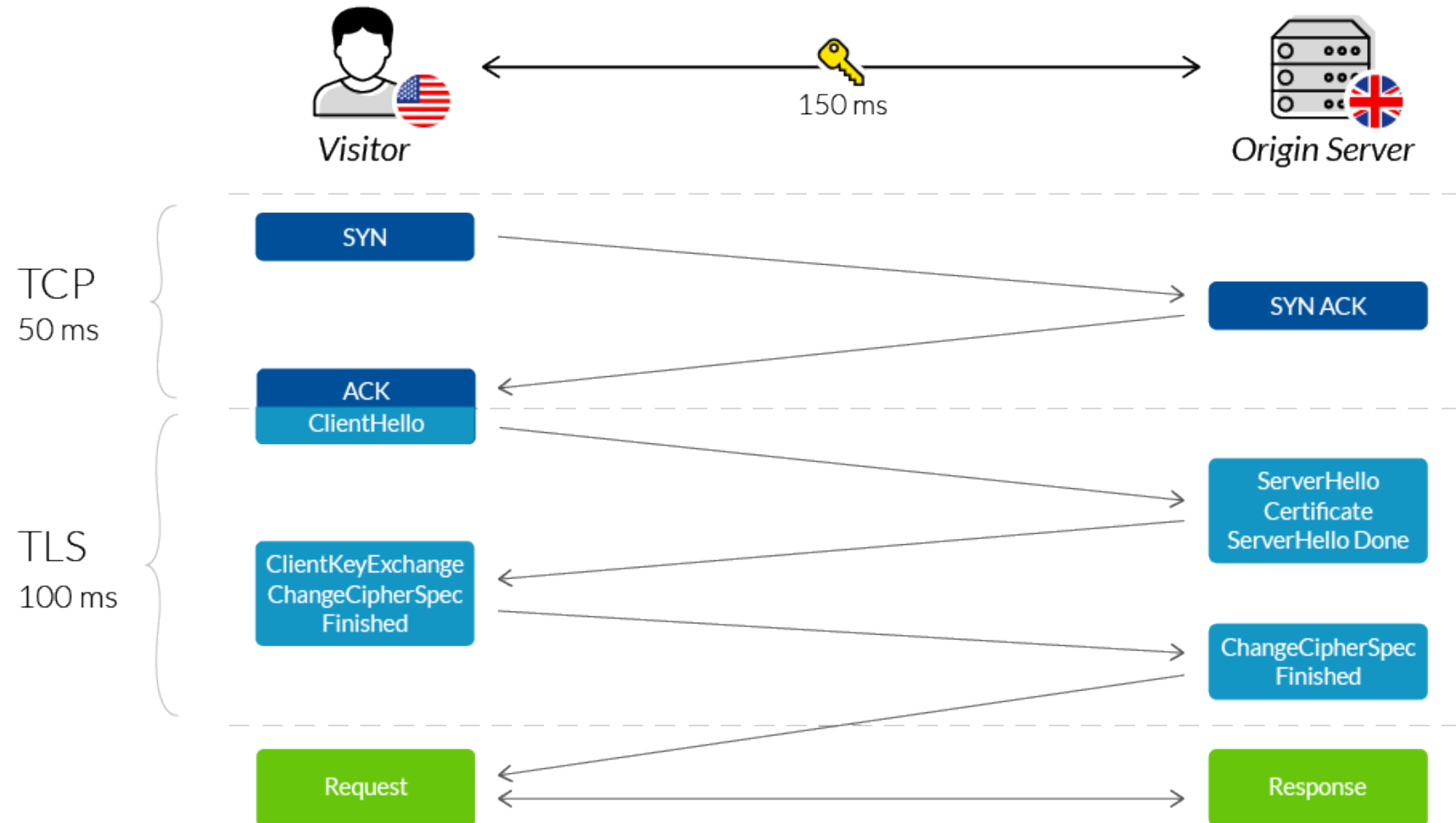
- Asimetrik şifreleme algoritmasıdır. Genel ve özel anahtar üretmek için kullanılır.
- Çok büyük asal sayılar kullanılmaktadır.
- Anahtar paylaşım sorunu yoktur.
- Simetrik şifreleme algoritmalarına kıyasla oldukça yavaştır.

Certificate Authority - CA

- Sertifika verme yetkisine sahip güvenilir kuruluştur. Bazıları;



SSL / TLS Diagram



SSL / TLS Trafiği

| No. | Time | Source | Destination | Protocol | Length | Info |
|------|---------------|--------------|--------------|----------|--------|---|
| 215 | 12.603789763 | 192.168.1.51 | 93.187.67.10 | TLSv1.2 | 259 | Client Hello |
| 217 | 12.656700634 | 93.187.67.10 | 192.168.1.51 | TLSv1.2 | 1506 | Server Hello |
| 223 | 12.702972713 | 93.187.67.10 | 192.168.1.51 | TLSv1.2 | 505 | Certificate, Server Key Exchange, Server Hello Done |
| 225 | 12.707532272 | 192.168.1.51 | 93.187.67.10 | TLSv1.2 | 192 | Client Key Exchange, Change Cipher Spec, Hello Request, Hello Request |
| 230 | 12.778015303 | 93.187.67.10 | 192.168.1.51 | TLSv1.2 | 72 | Change Cipher Spec |
| 233 | 12.783130816 | 93.187.67.10 | 192.168.1.51 | TLSv1.2 | 111 | Encrypted Handshake Message |
| 242 | 13.063479057 | 192.168.1.51 | 93.187.67.10 | TLSv1.2 | 415 | Application Data |
| 244 | 13.120965640 | 93.187.67.10 | 192.168.1.51 | TLSv1.2 | 286 | Application Data |
| 4279 | 128.293959204 | 192.168.1.51 | 93.187.67.10 | TLSv1.2 | 97 | Encrypted Alert |

Client Hello

- ▶ Internet Protocol Version 4, Src: 192.168.1.51, Dst: 93.187.67.10
- ▶ Transmission Control Protocol, Src Port: 59530, Dst Port: 443, Seq: 1, Ack: 1, Len: 193
- ▼ Secure Sockets Layer
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.0 (0x0301)
 - Length: 188
 - ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 184
 - Version: TLS 1.2 (0x0303)
 - ▶ Random
 - Session ID Length: 0
 - Cipher Suites Length: 30
 - ▼ Cipher Suites (15 suites)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
 - Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
 - Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
 - Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)

Client Hello 2

- ▶ Extension: status_request
- ▼ Extension: signature_algorithms
 - Type: signature_algorithms (0x000d)
 - Length: 24
 - Signature Hash Algorithms Length: 22
 - ▼ Signature Hash Algorithms (11 algorithms)
 - ▼ Signature Hash Algorithm: 0x0403
 - Signature Hash Algorithm Hash: SHA256 (4)
 - Signature Hash Algorithm Signature: ECDSA (3)
 - ▼ Signature Hash Algorithm: 0x0503
 - Signature Hash Algorithm Hash: SHA384 (5)
 - Signature Hash Algorithm Signature: ECDSA (3)
 - ▼ Signature Hash Algorithm: 0x0603
 - Signature Hash Algorithm Hash: SHA512 (6)
 - Signature Hash Algorithm Signature: ECDSA (3)
 - ▶ Signature Hash Algorithm: 0x0804
 - ▶ Signature Hash Algorithm: 0x0805
 - ▶ Signature Hash Algorithm: 0x0806
 - ▶ Signature Hash Algorithm: 0x0401
 - ▼ Signature Hash Algorithm: 0x0501
 - Signature Hash Algorithm Hash: SHA384 (5)
 - Signature Hash Algorithm Signature: RSA (1)
 - ▼ Signature Hash Algorithm: 0x0601
 - Signature Hash Algorithm Hash: SHA512 (6)
 - Signature Hash Algorithm Signature: RSA (1)
 - ▼ Signature Hash Algorithm: 0x0203
 - Signature Hash Algorithm Hash: SHA1 (2)
 - Signature Hash Algorithm Signature: ECDSA (3)
 - ▶ Signature Hash Algorithm: 0x0201

Server Hello

- ▼ Secure Sockets Layer

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello

- Content Type: Handshake (22)

- Version: TLS 1.2 (0x0303)

- Length: 87

- ▼ Handshake Protocol: Server Hello

- Handshake Type: Server Hello (2)

- Length: 83

- Version: TLS 1.2 (0x0303)

- ▶ Random

- Session ID Length: 32

- Session ID: 016ddb7ec5613e93c895561a0d08c77baa81aed783702bfa...

- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

- Compression Method: null (0)

- Extensions Length: 11

- ▼ Extension: renegotiation_info

- Type: renegotiation_info (0xff01)

- Length: 1

- ▶ Renegotiation Info extension

- ▼ Extension: ec_point_formats

- Type: ec_point_formats (0x000b)

- Length: 2

- EC point formats Length: 1

- ▶ Elliptic curves point formats (1)

Server Certificate

```
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Certificate
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 4315
      Handshake Protocol: Certificate
        Handshake Type: Certificate (11)
        Length: 4311
        Certificates Length: 4308
          Certificates (4308 bytes)
            Certificate Length: 1720
            ▶ Certificate: 308206b43082059ca00302010202107ef50689e6094e303b... (id-at-commonName=*.gittigidiyor.com,id-at-organizationalUnitName=Technology & Product,id-at-organizationalUnitName=Technology & Product,CN=*.gittigidiyor.com)
            Certificate Length: 1340
            ▶ Certificate: 3082053830820420a0030201020210513fb9743870b73440... (id-at-commonName=Symantec Class 3 Secure Server CA - G4,id-at-organizationalUnitName=Symantec Trust Network,id-at-organizationalUnitName=Symantec Trust Network,CN=Symantec Class 3 Secure Server CA - G4)
            Certificate Length: 1239
            ▶ Certificate: 308204d3308203bba003020102021018dad19e267de8bb4a... (id-at-commonName=VeriSign Class 3 Public Primary Certification Authority,id-at-organizationalUnitName=VeriSign Class 3 Public Primary Certification Authority,CN=VeriSign Class 3 Public Primary Certification Authority)
```

Key Exchange

- ▼ Secure Sockets Layer

- ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Key Exchange

- Content Type: Handshake (22)

- Version: TLS 1.2 (0x0303)

- Length: 333

- ▼ Handshake Protocol: Server Key Exchange

- Handshake Type: Server Key Exchange (12)

- Length: 329

- ▼ EC Diffie-Hellman Server Params

- Curve Type: named_curve (0x03)

- Named Curve: secp256r1 (0x0017)

- Pubkey Length: 65

- Pubkey: 045d0c5eedec3599af01ffa42e8cc0a17b108d5d31ca9327...

- ▶ Signature Hash Algorithm: 0x0401

- Signature Length: 256

- Signature: 85984cb4225f7129312d91a26ba2a897fb72fb348e35d6ed...

- ▼ 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

Şifreli Veri

| | | | | | |
|------|---------------|--------------|--------------|---------|----------------------|
| 242 | 13.063479057 | 192.168.1.51 | 93.187.67.10 | TLSv1.2 | 415 Application Data |
| 244 | 13.120965640 | 93.187.67.10 | 192.168.1.51 | TLSv1.2 | 286 Application Data |
| 4279 | 128.293959204 | 192.168.1.51 | 93.187.67.10 | TLSv1.2 | 97 Encrypted Alert |

| | |
|---|---|
| ▶ | Frame 242: 415 bytes on wire (3320 bits), 415 bytes captured (3320 bits) on interface 0 |
| ▶ | Ethernet II, Src: IntelCor_7d:79:81 (0c:8b:fd:7d:79:81), Dst: ZyxelCom_25:86:4e (e8:37:7a:25:86:4e) |
| ▶ | Internet Protocol Version 4, Src: 192.168.1.51, Dst: 93.187.67.10 |
| ▶ | Transmission Control Protocol, Src Port: 59530, Dst Port: 443, Seq: 320, Ack: 4811, Len: 349 |
| ▼ | Secure Sockets Layer |
| ▼ | TLSv1.2 Record Layer: Application Data Protocol: http-over-tls |
| | Content Type: Application Data (23) |
| | Version: TLS 1.2 (0x0303) |
| | Length: 344 |
| | Encrypted Application Data: 0000000000000000154290cf416298b51d4a314d7c053b2d9... |

| | | | |
|------|-------------------------|-------------------------|--------------------|
| 0010 | 01 91 00 20 40 00 40 06 | d6 a6 c0 a8 01 33 5d bb | ... @.@.3]. |
| 0020 | 43 0a e8 8a 01 bb d8 33 | 44 96 4b 98 a8 1a 80 18 | C.....3 D.K..... |
| 0030 | 9d 80 73 1c 00 00 01 01 | 08 0a 13 12 a6 1f 3d 04 | ..s.....=. |
| 0040 | 42 2a 17 03 03 01 58 00 | 00 00 00 00 00 00 01 54 | B*....X.T |
| 0050 | 29 0c f4 16 29 8b 51 d4 | a3 14 d7 c0 53 b2 d9 57 |)...).Q.S..w |
| 0060 | e3 8e ef 11 c9 6a 98 44 | 0f fd d3 22 9d bd ed c7 |j.D".... |
| 0070 | 93 8d b7 6c 9a a9 2f 92 | 7a 39 79 1b a6 e4 d2 30 | ...l../. z9y....0 |
| 0080 | 98 b8 df 25 8f 98 3c cc | 88 18 ee 63 3e 77 d7 5a | ...%...<. ...c>w.Z |
| 0090 | 84 e9 ce ae 8f 71 9a e7 | b6 d4 ee 92 4e 2a 24 bf |q..N*\$. |
| 00a0 | 0c d5 64 58 4d 4f b5 61 | b5 01 ac c8 d3 31 bc 00 | ..dXM0.a1.. |
| 00b0 | 77 16 9d cf 4b 9a 3a ac | a3 2e 4d be 4b 8b 95 14 | w...K.:. ..M.K... |
| 00c0 | 80 b5 e5 47 c2 0d 3a 37 | 1e 12 c5 fb 9b 04 7f e4 | ...G...:7 |
| 00d0 | 50 1c 82 cc 40 75 13 33 | cb a5 4e b7 5a 63 c7 46 | P...@u.3 ..N.Zc.F |
| 00e0 | b3 82 2a d9 43 2f a3 15 | 7b 8a a7 e3 4d ce 0f 6b | ..*.C/.. {...M..k |
| 00f0 | 48 a3 72 95 b3 7c 8b e5 | c6 9d ee fe c7 45 2c c3 | H.r...E,. |
| 0100 | 9b 00 3a 94 e7 8c cc ca | d9 6a f0 90 05 cf 12 dd | ...:..... .j..... |
| 0110 | 20 c1 34 31 e7 56 61 e0 | e7 23 64 55 96 2b 7b 4f | .41.Va. .#dU.+{0 |
| 0120 | 32 c8 3f ca fa 8c 63 f5 | 3d 23 8d 5c ac a3 49 4b | 2.?...c. =#\..IK |
| 0130 | 88 3d 8f 70 04 ab 2e 92 | ba 8c bf 86 23 f4 f1 0f | ..=p....#... |
| 0140 | e1 f4 a6 f3 75 5f 4c 77 | 31 50 88 15 f2 63 66 00 |u_Lw 1P...cf. |
| 0150 | 24 e0 5b 09 17 13 37 55 | a8 a4 fc ca f8 92 db 99 | \$. [...7U |
| 0160 | 0f 37 c8 fa 68 7d d5 4d | 8f f9 7c be 5f a7 b1 6b | .7..h}.M .. _..k |
| 0170 | 1a 86 f6 98 7a c9 3b ad | ab 16 8f b0 d2 5a cb 41 |z.;.Z.A |
| 0180 | d4 e2 6b f0 d6 0e 3f 77 | 85 71 71 e9 00 94 01 4f | ..k...?w .qq....0 |
| 0190 | bc 7b 39 d0 89 21 94 4c | 06 73 12 0c 0b a0 3e | .{9...!..L .s....> |

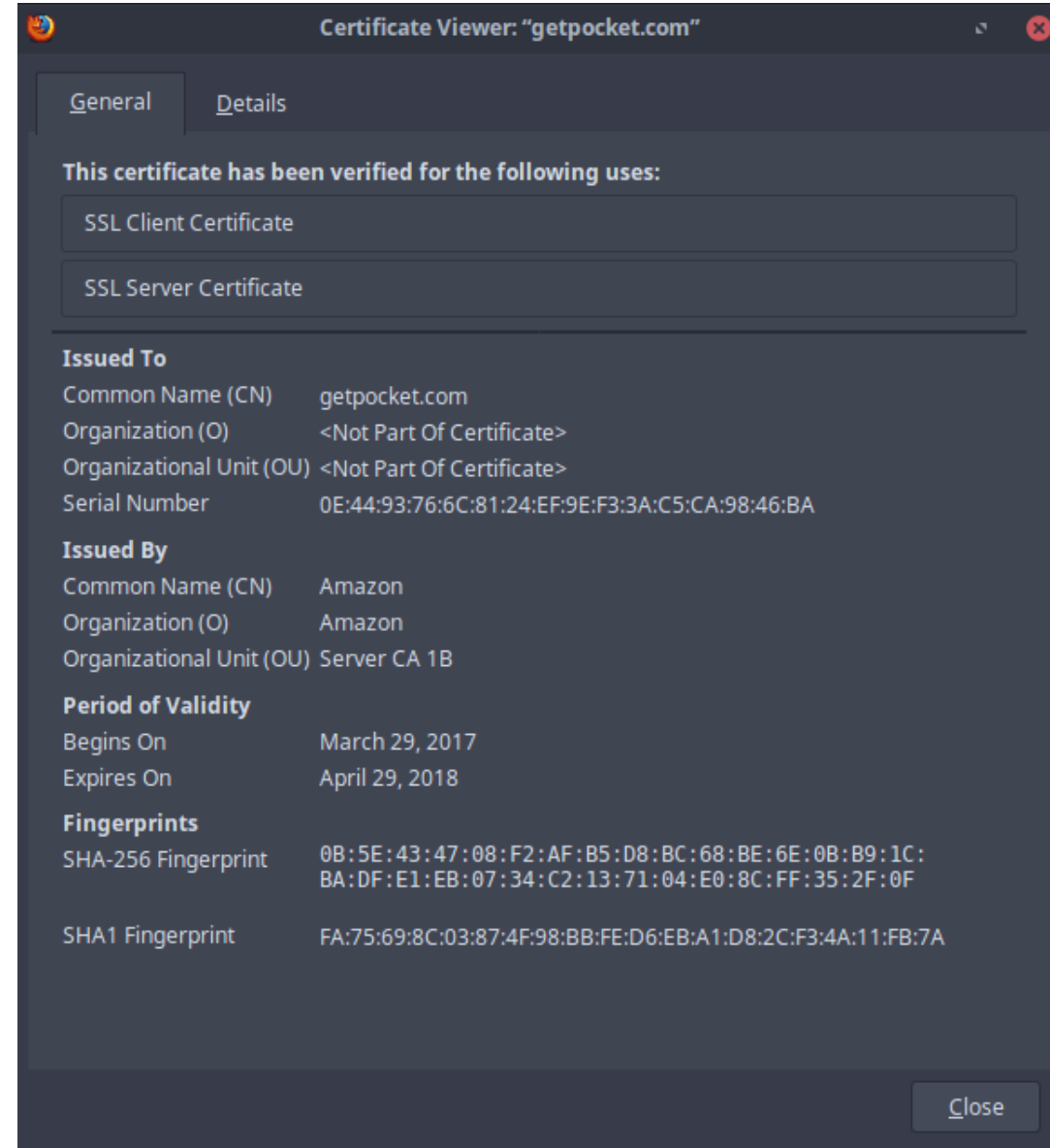
Sertifika neden ihtiyaç var ?



- Kişi/kurumun gerçekliğini teyit eden ve kullanılan public anahtarın gerçekten ilgili kişi/kuruma ait olduğunu doğrulayan dijital veriler bütünüdür.

Sertifika Türleri

1) Domain Validation(DV)

Sadece alan adı doğrulaması yapan sertifika türüdür.

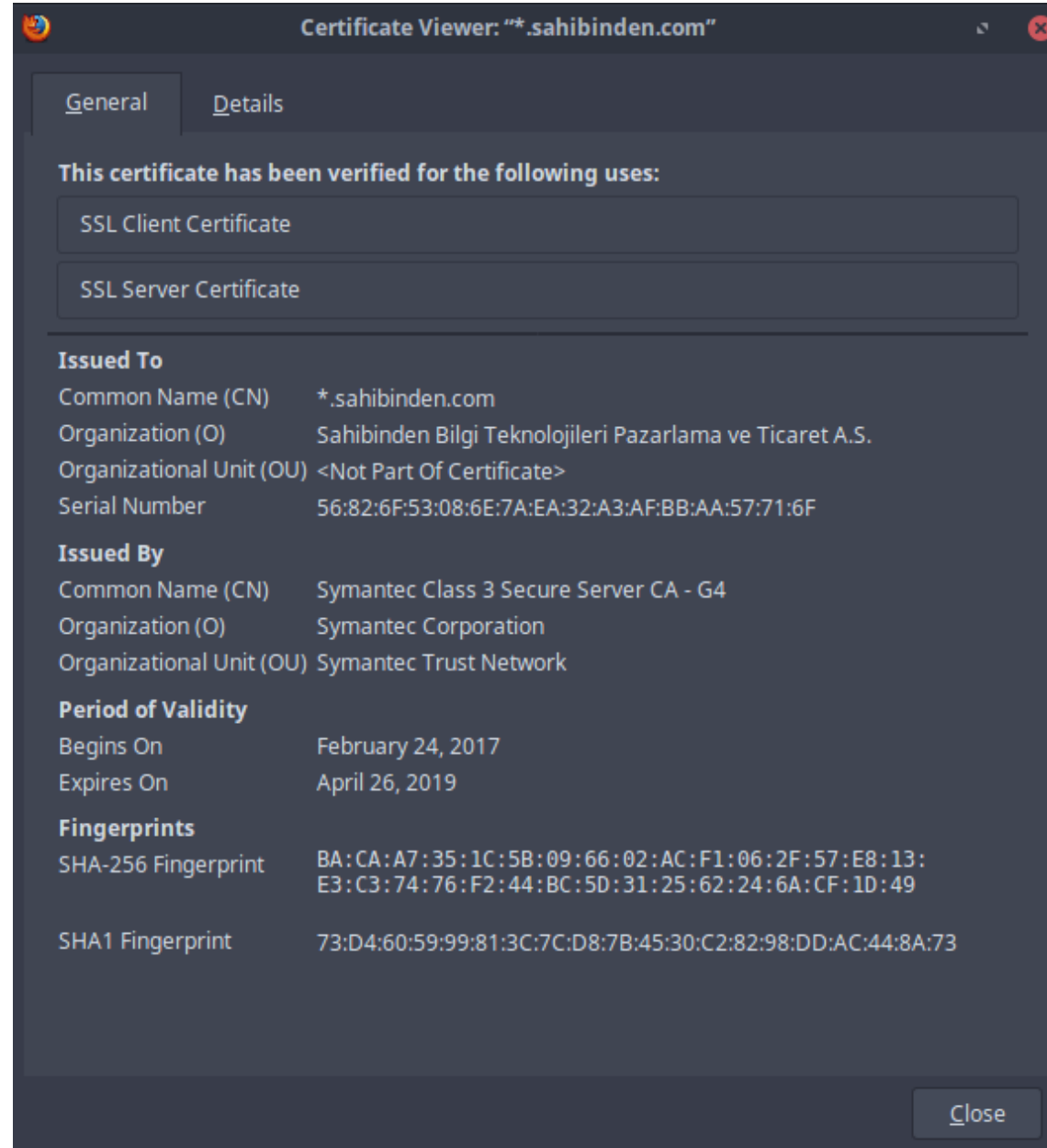




  https://getpocket.com/a/queue/

Sertifika Türleri

- 2) **Organizational Validation - OV**

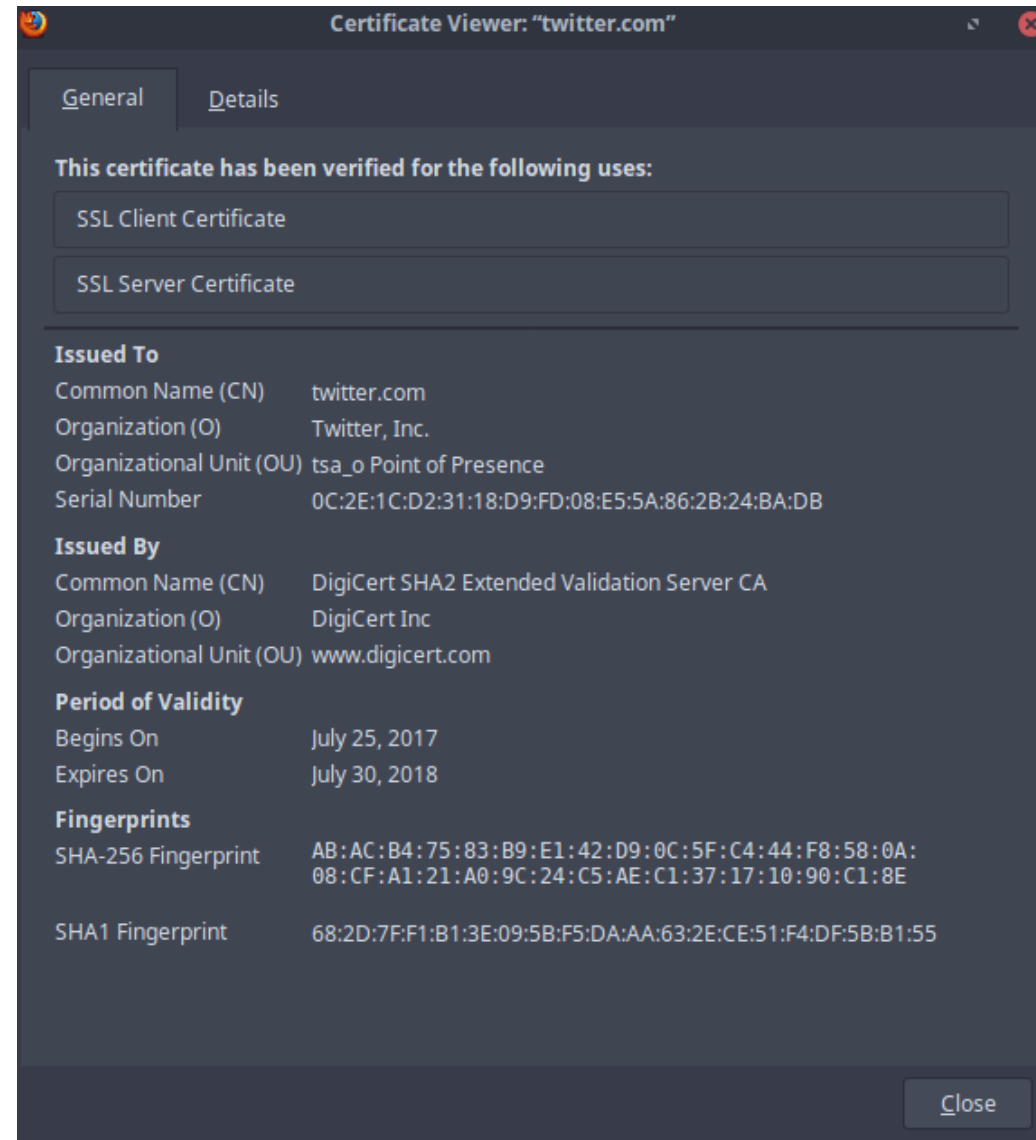
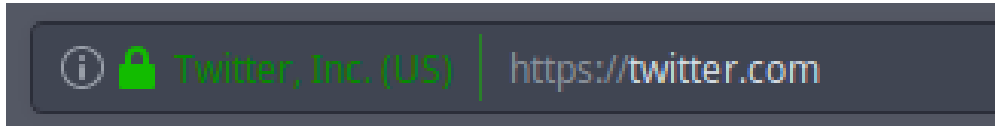
Bir firmaya ait (firma ismi, başvurunun firmadan çalışan bir kişi tarafından geldiği vs.) bilgileri doğrulayan sertifika türüdür.



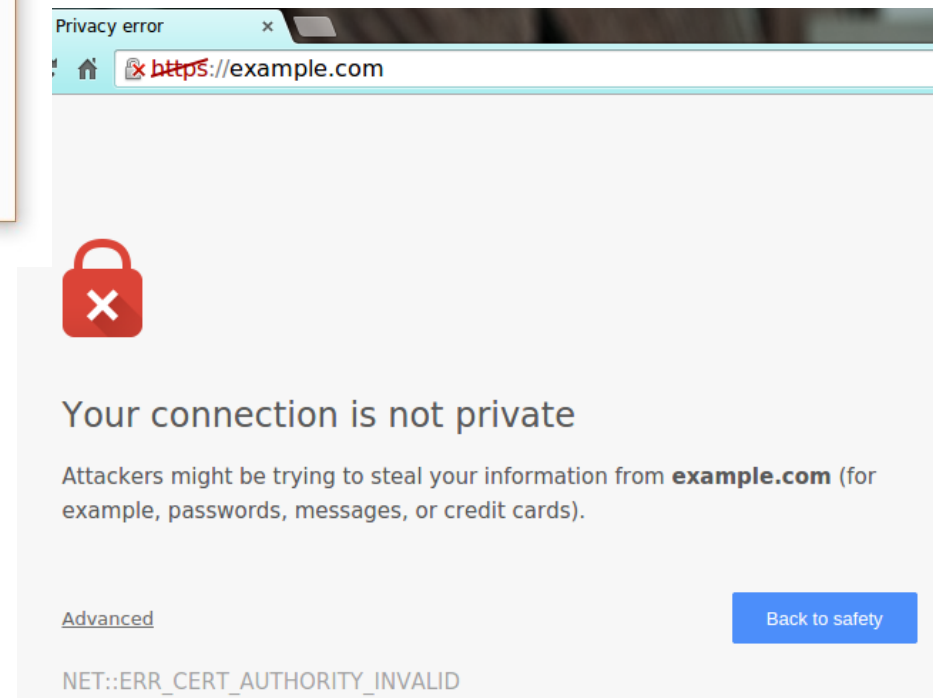
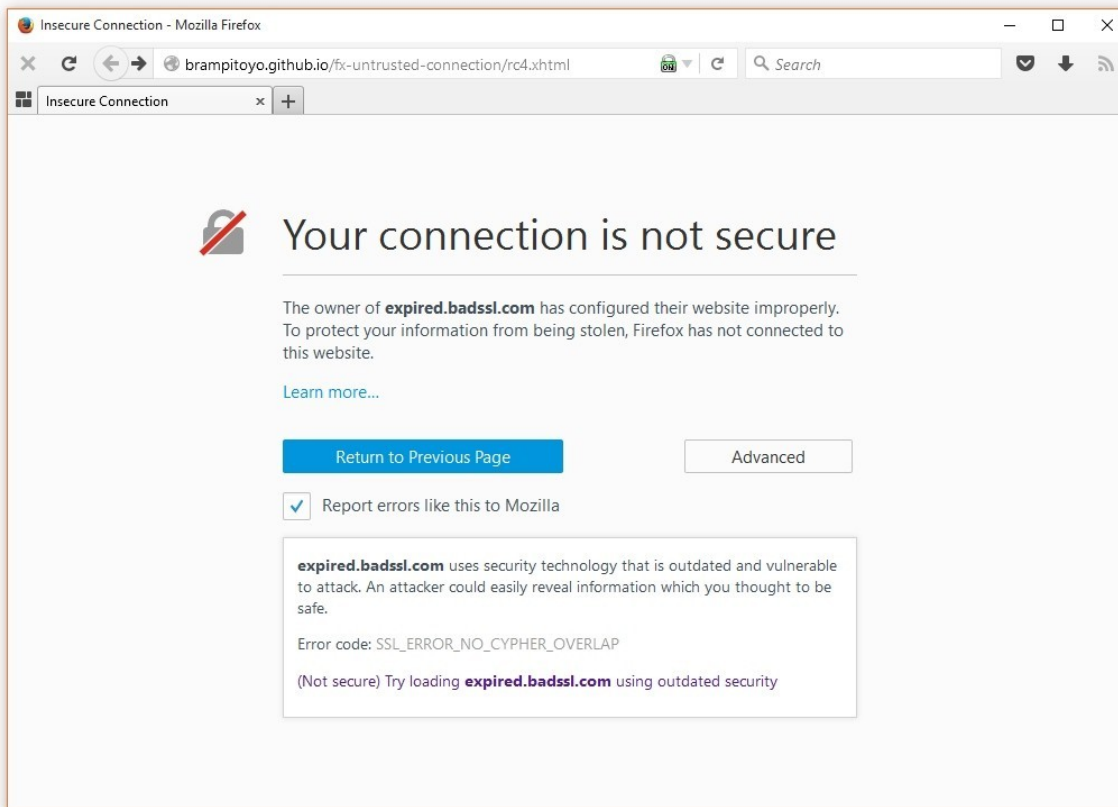
  <https://www.sahibinden.com>

Sertifika Türleri

- **Extended Validation – EV:** Firmaların çok kapsamlı bir şekilde fiziksel, hukuksal ve ticari varlıklarını doğrulayan sertifika türüdür.
- Yeşil asma kilitin yanında firmanın kurumsal ismide yer alır.
- En pahalı sertifika türüdür.

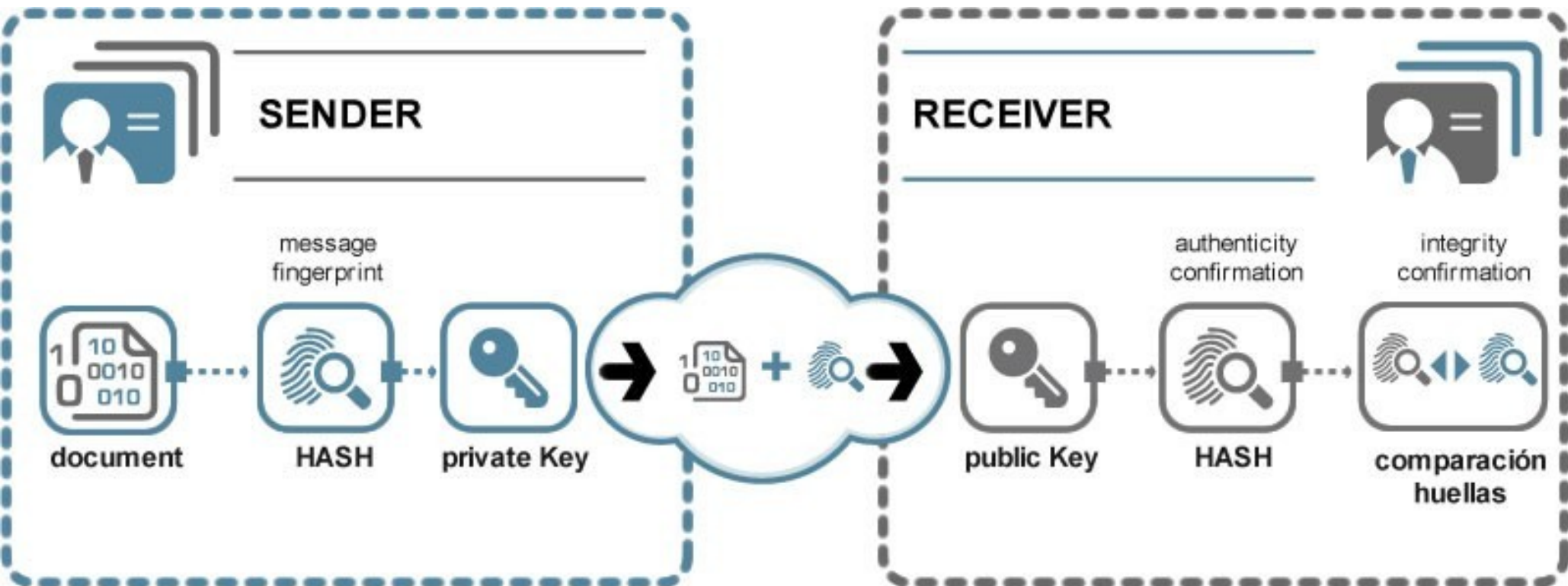


SSL / TLS Hataları

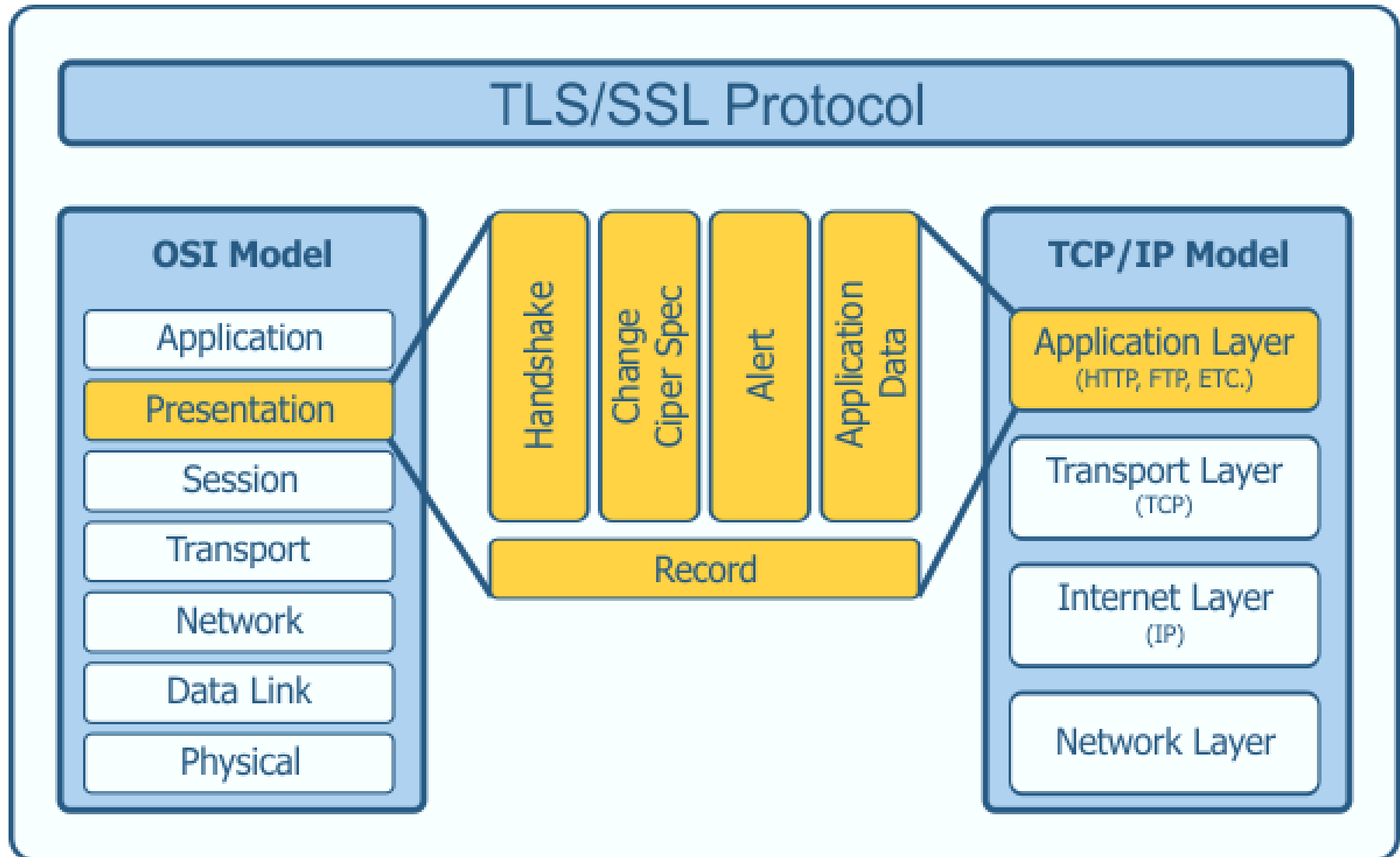


Doğrulama & Bütünlük

- Mesajın doğru kişiden geldiği nasıl doğrulanmaktadır ?
- Gönderilecek mesajın hash değeri alınır daha sonra bu değer private key ile Şifrelenerek karşıya gönderilir. Karşı taraf gelen şifreli veriyi (hash) decrypt etmek için public key'i kullanır ve hash değerine ulaşır.
- Daha öncesinden aldığı mesajın hash değeri ile decrypt ettiği hash değerini Karşılaştırarak mesajın doğru kişiden geldiğini ve arada bir yerlerde değiştirilmediğinden emin olur.

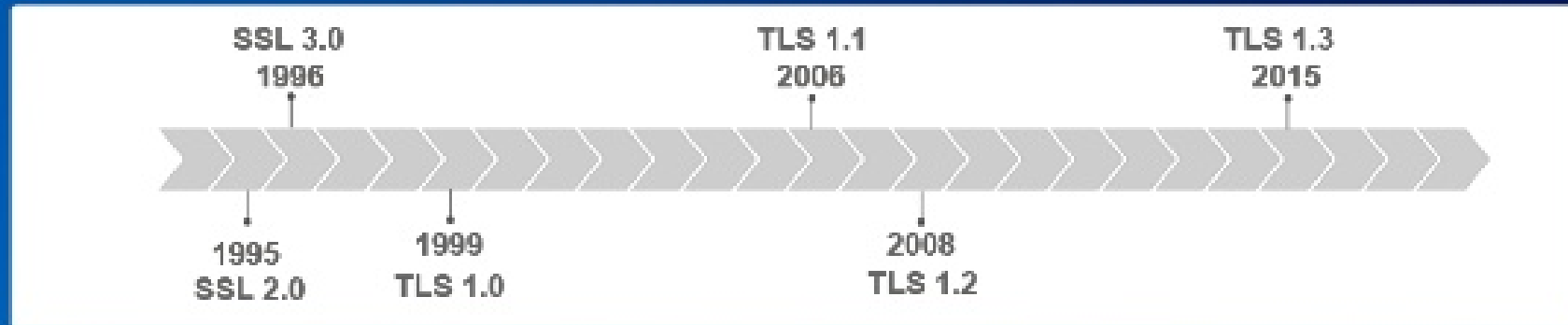


Şifreli paket router tarafından nasıl yönlendirilir ?



Geçmişten Bugüne SSL/TLS

History of SSL / TLS



- *SSL (Secured Socket Layers)*
 - First version: Netscape in 1994
 - SSL 2.0: 1995
 - SSL 3.0: 1996
- IETF standardization: *TLS (Transport Layer Security)*
 - TLS 1.0: 1999 (based on SSL 3.0)
 - TLS 1.1: 2006
 - TLS 1.2: 2008
 - TLS 1.3: 2015

SSL/TLS'e yönelik Saldırılar

- BEAST (CVE-2011-3389)

SSL 3.0 ve öncesini etkilenmiştir.

- POODLE (CVE-2014-3566)

SSLv3.0 ve TLS 1.0' ı etkilemiştir.

- SSLStrip

Bağlantıyı downgrade ederek yapılan saldırı tekniğidir.

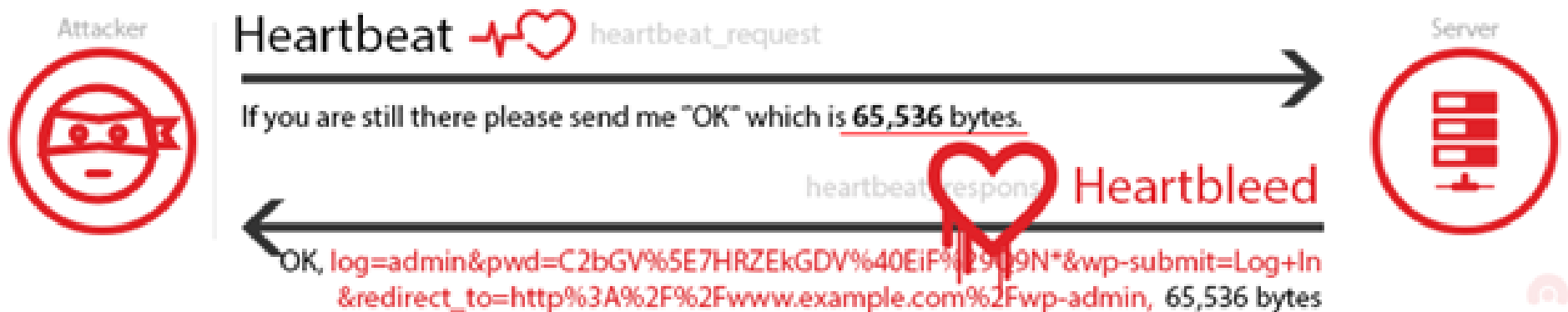
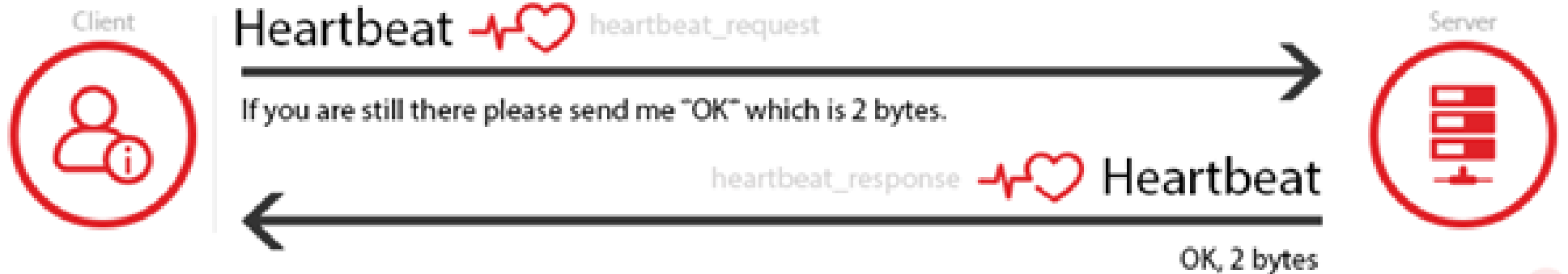
beast

poodle



HeartBleed

OpenSSL kütüphanesinde kullanılan bir metoda beklediğinden fazla bir değer verilmesi halinde veri sızıntısına sebep olan bir zafiyettir. 2014 yılında farkedilmiştir.



Bonus + :

Ücretsiz SSL/TLS Sertifikası:

Let's Encrypt