Perfectionist's Guide To

TLS Optimizations & HTTP Headers

Ayesh Karunaratne | https://ayesh.me/talk/TLS-HTTP-Headers


Deutsche Post
Deutsche Post
Deutsche Post

How do you mail a parcel securely and fast?

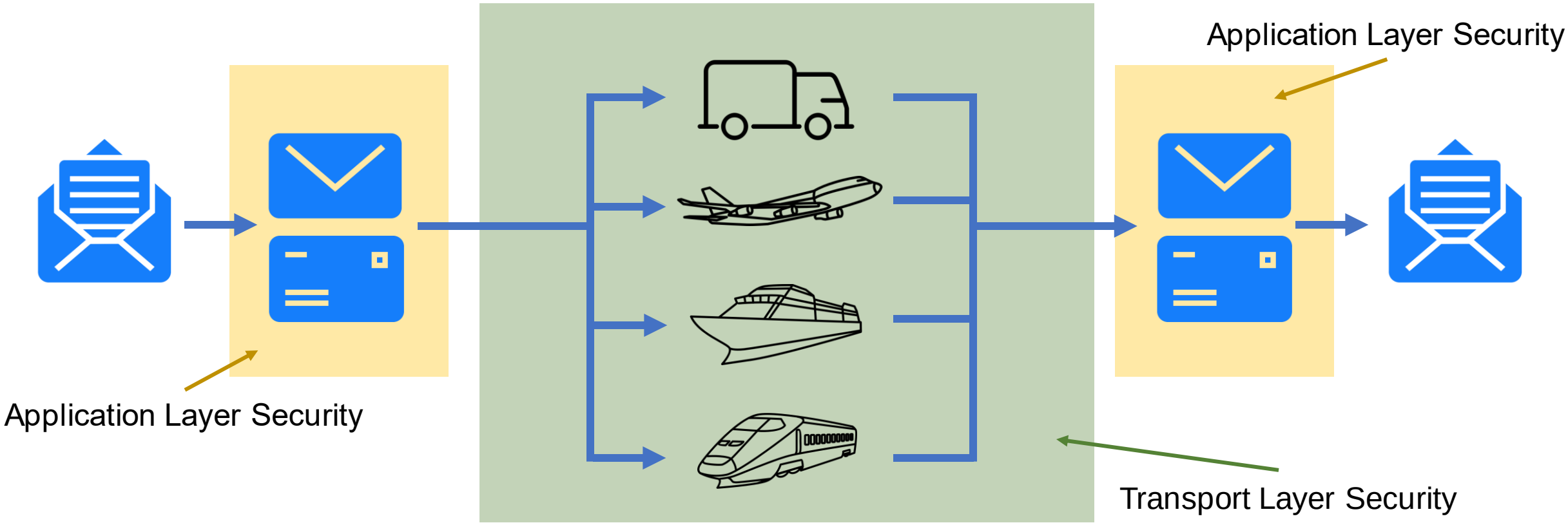
How do you mail a parcel securely and fast?

How do you mail a parcel **securely** and **fast**?

How do you mail a parcel **securely** and **fast**?

How do you mail a parcel **securely** and **fast**?

How do you mail a parcel **securely** and **fast**?



How do **serve web sites securely** and **fast**?

HTTPS
(TLS/SSL)

HTTP
Headers

Perfectionist's Guide to HTTPS Optimizations & HTTP Headers

Hello

Здравейте

Ayesh Karunaratne

Freelance Software Developer, Security Researcher, Full-time traveler

Kandy, Sri Lanka - Everywhere

https://ayesh.me

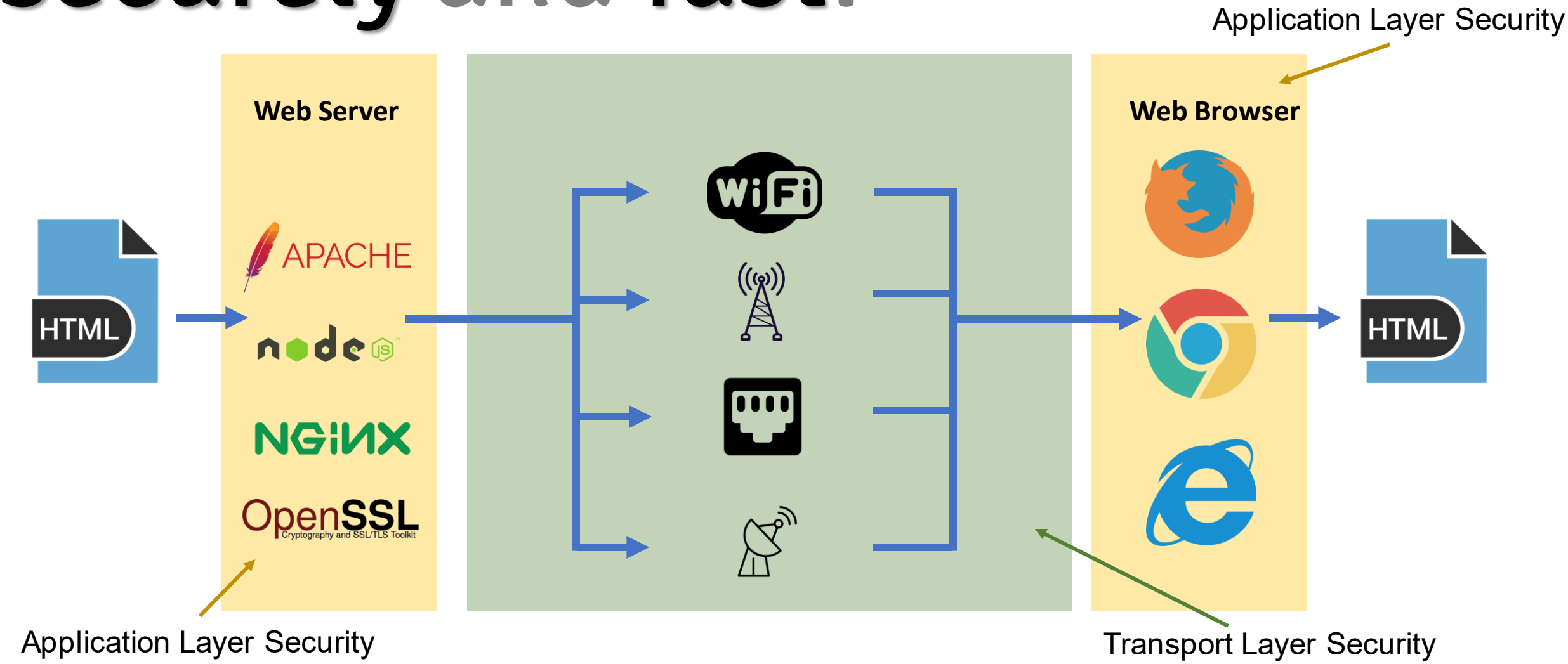
Ayesh

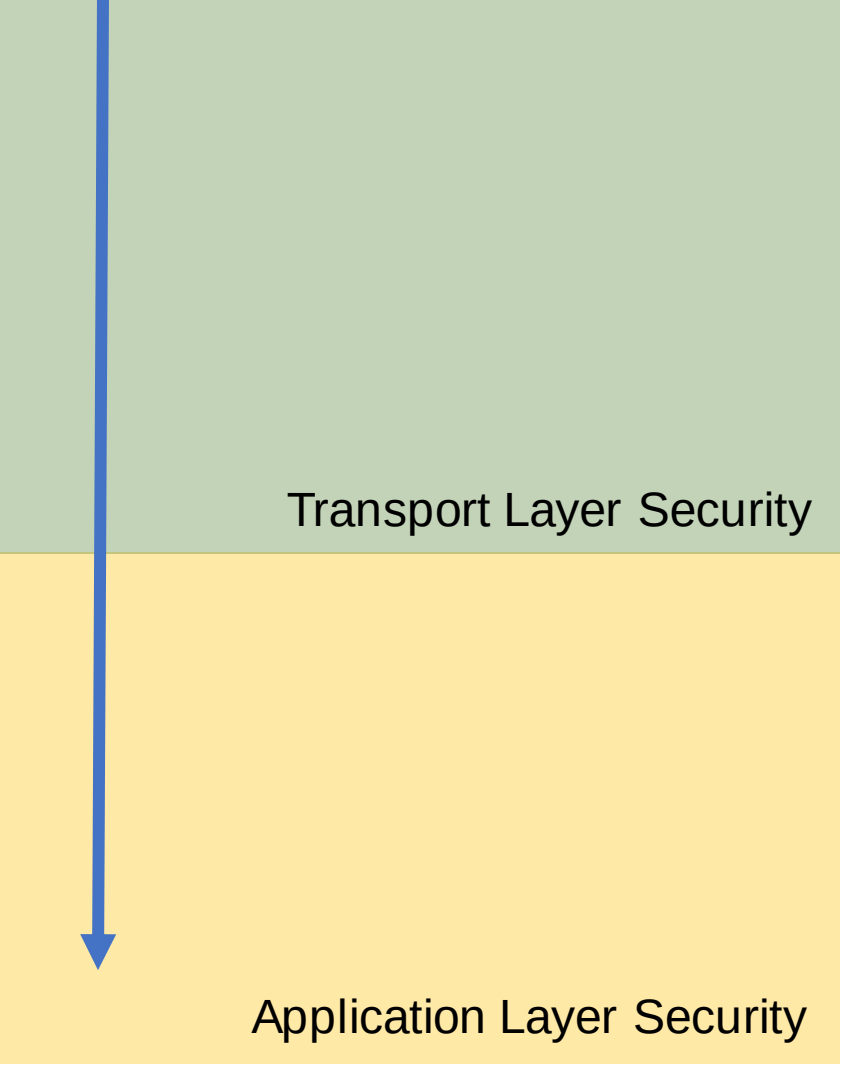
@Ayeshlive

Ayesh

Perfectionist's Guide to HTTPS Optimizations & HTTP Headers

How do serve web sites securely and fast?





Authentication The server is what it says it is

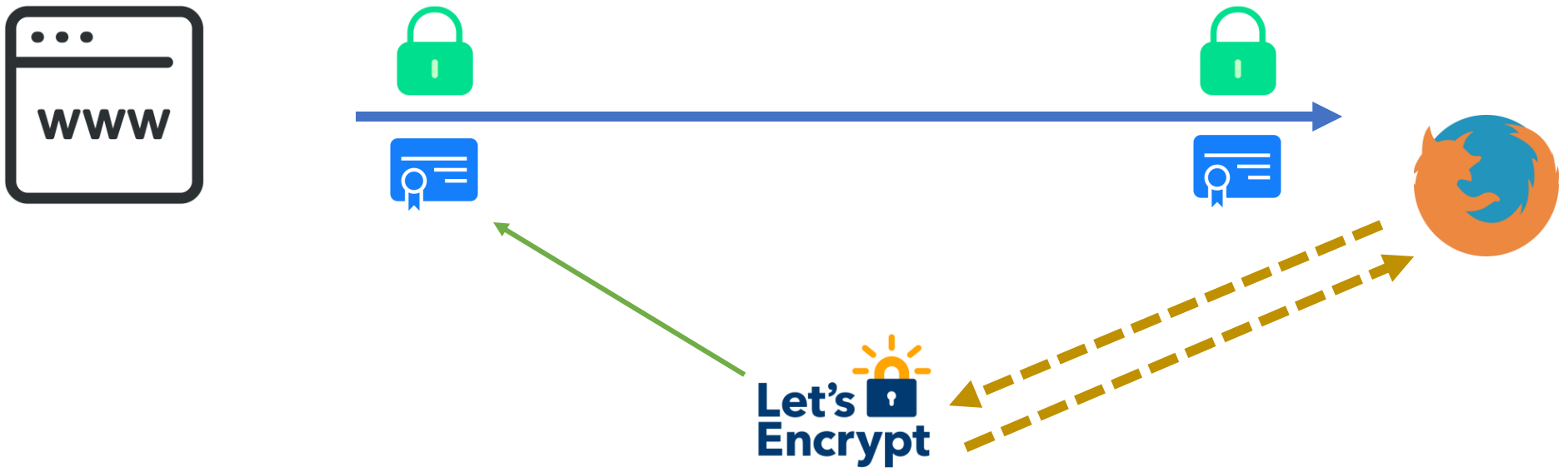
Private Nobody can see what is being transferred

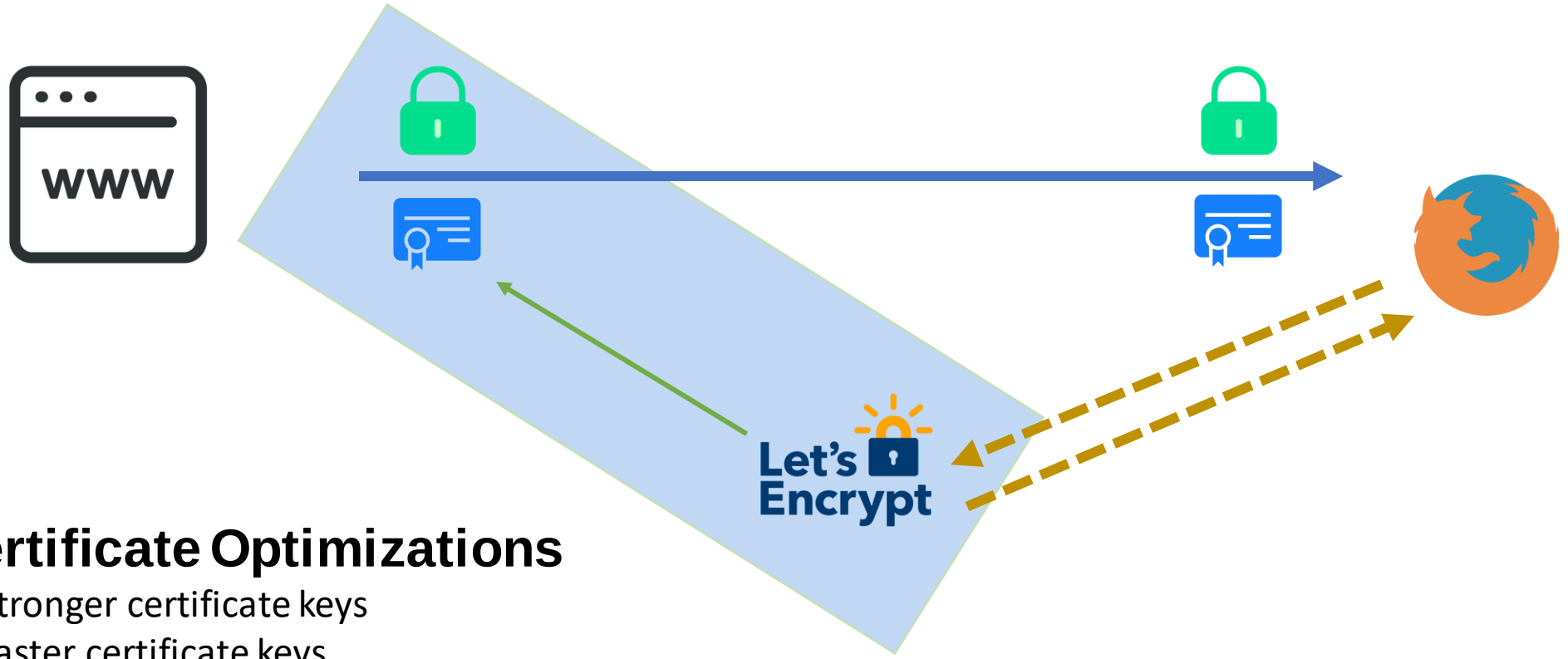
Untampered Nobody can change what is being transferred

Authorization Who can access this data

Behavior How the page is allowed to behave

Authenticity How to validate authenticity of the data


www
Let's Encrypt

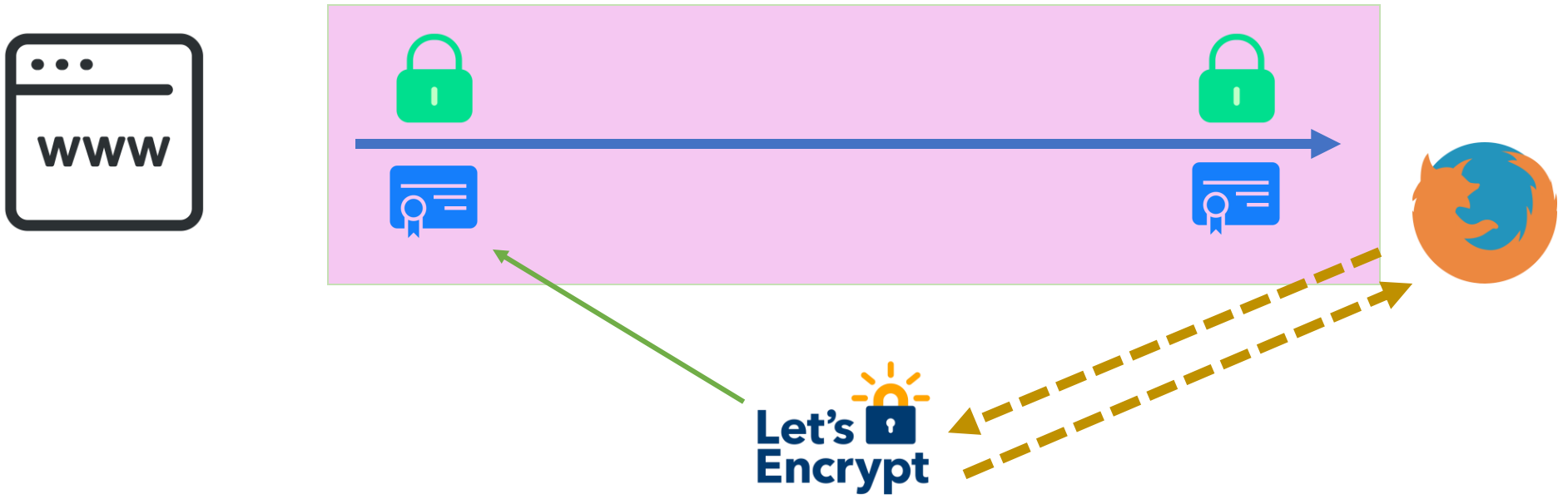


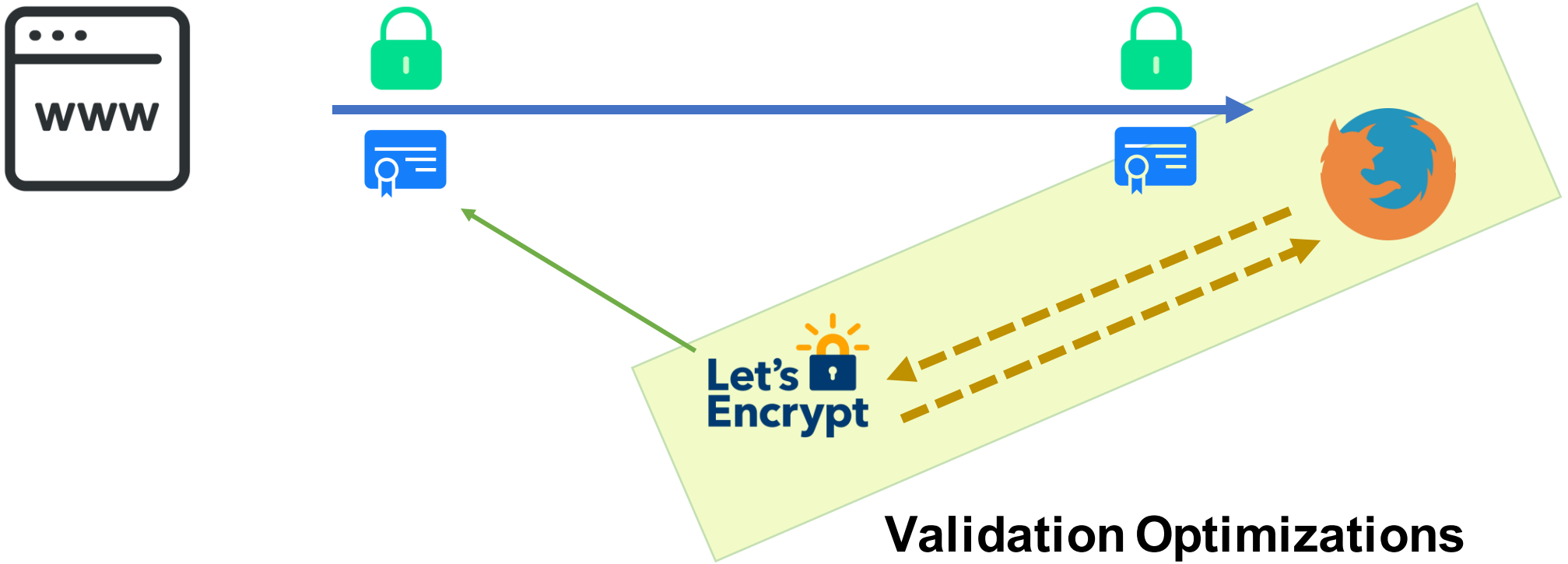
Certificate Optimizations

- Stronger certificate keys
- Faster certificate keys
- Smaller certificates

Encryption and Handshake Optimizations

- Stronger cryptographic strength
- Faster encryption algorithms
- Better protocols





Validation Optimizations

- Eliminate the need for them with short-lived certificates
- Staple OCSP information
- Embed Certificate Transparency Info

Certificate Optimizations

Certificate Optimizations

Let's Encrypt

SECTIGO

digicert

Entrust Datacard

RSA

This certificate authenticates
example.com, www.example.com

Valid from
15 Jan 2019 to 15 Apr 2019

Public key algorithm
RSA-2048 bits

Public key
…c2 04 ec f8 8c ee 04 …

Certificate Optimizations

Let's Encrypt

SECTIGO

digicert

Entrust Datacard

RSA

This certificate authenticates
example.com, www.example.com

Valid from
15 Jan 2019 to 15 Apr 2019

Public key algorithm
RSA-2048 bits

Public key
…c2 04 ec f8 8c ee 04 …
2048 bits

ECC

This certificate authenticates
example.com, www.example.com

Valid from
15 Jan 2019 to 15 Apr 2019

Public key algorithm
prime256v1: 256 bits

Public key
…04 f1 a3 ff 46 e9 …
256 bits

Certificate Optimizations

Let's Encrypt

SECTIGO

digicert

Entrust Datacard

RSA

This certificate authenticates
example.com, www.example.com

Valid from
15 Jan 2019 to 15 Apr 2019

Public key algorithm
RSA-2048 bits

Public key
…c2 04 ec f8 8c ee 04 …
2048 bits

ECC

This certificate authenticates
example.com, www.example.com

Valid from
15 Jan 2019 to 15 Apr 2019

Public key algorithm
prime256v1: 256 bits

Public key
…04 f1 a3 ff 46 e9 …
256 bits

Certificate Optimizations

`openssl speed`

RSA	2048 bit keys	1002.6 sign/sec	33885 verify/sec
	4096 bit keys	162 sign/sec	10860 verify/sec
ECC	256 bit keys	13275.6 sign/sec	6801.1 verify/sec
	384 bit keys	2572.4 sign/sec	658.1 verify/sec

Certificate Optimizations

Serve RSA + ECC certificates from the web server


```
<VirtualHost *:443>
  SSLEngine on
  ...
  SSLCertificateFile /path/to/rsa.pem
  SSLCertificateKeyFile /path/to/rsa.key.pem

  SSLCertificateFile /path/to/ecc.pem
  SSLCertificateKeyFile /path/to/ecc.key.pem
  ...
</VirtualHost>
```


```
server {
  ssl_certificate /path/to/rsa.pem;
  ssl_certificate_key /path/to/rsa.key.pem;

  ssl_certificate /path/to/ecc.key.pem
  ssl_certificate_key /path/to/ecc.key.pem
}
```

Encryption and Handshake Optimizations

Encryption and Handshake Optimizations

Cipher Suites

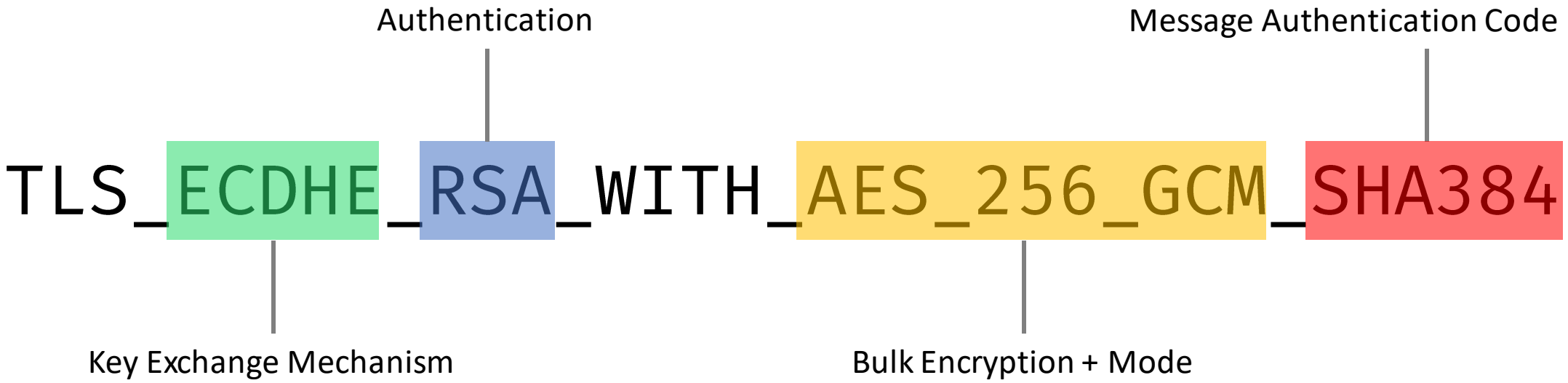
A set of algorithms that help secure a network connection that uses Transport Layer Security

TLS Versions

A well-defined protocol that defines cipher suites and other encryption mechanisms that servers and user agents agree to.

Encryption and Handshake Optimizations

Cipher Suites



Encryption and Handshake Optimizations

Cipher Suites

Insecure

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_RC4128_SHA
TLS_ECDHE_RSA_WITH_3DES_CBC_SHA
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA
TLS_DH_anon_WITH_AES_256_CBC_SHA
TLS_CK_RC4_64_WITH_MD5
TLS_DH_anon_EXPORT_WITHDES40_CBC_CBC_SHA
….

Weak MAC, no forward-secrecy, broken encryption

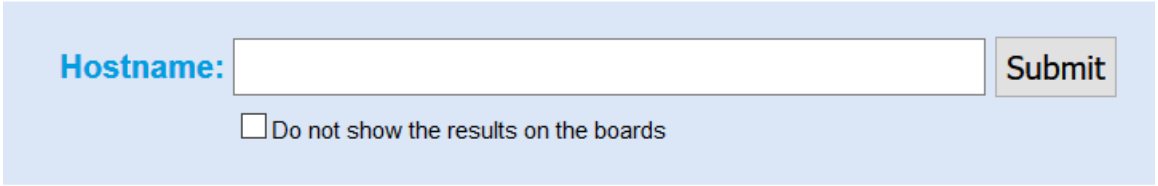
Secure and Faster

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
….

Forward-secrecy, low-cost encryption, hardware-acceleration

Encryption and Handshake Optimizations

Cipher Suites



https://www.ssllabs.com/ssltest/index.html

Encryption and Handshake Optimizations

Cipher Suites

Cipher Suites

 # TLS 1.3 (suites in server-preferred order)

TLS_CHACHA20_POLY1305_SHA256 (0x1303)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_AES_128_GCM_SHA256 (0x1301)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_AES_256_GCM_SHA384 (0x1302)	ECDH x25519 (eq. 3072 bits RSA) FS	256

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH x25519 (eq. 3072 bits RSA) FS	128
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)	ECDH x25519 (eq. 3072 bits RSA) FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x9e)	DH 2048 bits FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f)	DH 2048 bits FS	256

https://www.ssllabs.com/ssltest/index.html

Encryption and Handshake Optimizations

Cipher Suites

Cipher Suites

 # TLS 1.2 (suites in server-preferred order)

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x9f) DH 2048 bits FS	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x6b) DH 2048 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39) DH 2048 bits FS **WEAK**	256
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88) DH 2048 bits FS **WEAK**	256
TLS_ECDH_anon_WITH_AES_256_CBC_SHA (0xc019) **INSECURE**	256
TLS_DH_anon_WITH_AES_256_GCM_SHA384 (0xa7) **INSECURE**	256
TLS_DH_anon_WITH_AES_256_CBC_SHA256 (0x6d) **INSECURE**	256
TLS_DH_anon_WITH_AES_256_CBC_SHA (0x3a) **INSECURE**	256
TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA (0x89) **INSECURE**	256
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK**	256
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK**	256

https://www.ssllabs.com/ssltest/index.html

Encryption and Handshake Optimizations

Cipher Suites

moz://a

SSL Configuration Generator

Server Software

- Apache
- AWS ALB
- AWS ELB
- Caddy
- Dovecot
- Exim
- Golang
- HAProxy
- lighttpd
- MySQL
- (●) nginx
- Oracle HTTP
- Postfix
- PostgreSQL
- ProFTPD
- Traefik

Mozilla Configuration

- Modern
  Services with clients that support TLS 1.3 and don't need backward compatibility
- (●) Intermediate
  General-purpose servers with a variety of clients, recommended for almost all systems
- Old
  Compatible with a number of very old clients, and should be used only as a last resort

Environment

Server Version	1.17.0
OpenSSL Version	1.1.1c

Miscellaneous

- ☑ HTTP Strict Transport Security
  This also redirects to HTTPS, if possible
- ☑ OCSP Stapling

https://ssl-config.mozilla.org/

Encryption and Handshake Optimizations

Cipher Suites


```
SSLCipherSuite ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-
RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-
SHA384:ECDHE-RSA ...
```

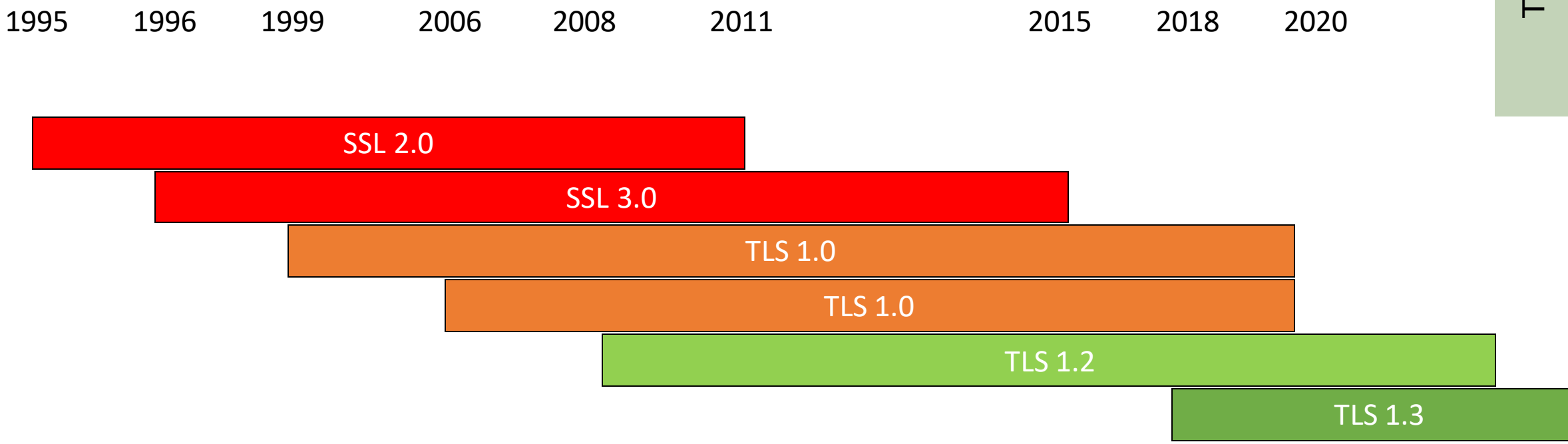

```
server {
  ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-
RSA-AES128-
}
```

Encryption and Handshake Optimizations

Transport Layer Security

Protocols

TLS Versions



Encryption and Handshake Optimizations

TLS Versions


```
SSLProtocol all -SSLv3 -TLSv1 -TLSv1.1
```

https://ayesh.me/TLSv1.3-Apache


```
server {
  ssl_protocols TLSv1.2 TLSv1.3
}
```

Certificate Validation

Certificate Validation

1. Certificate Authority is authorized to issue certificates
2. Certificate is valid and not revoked
3. Certificate Authorities are accounted for the certificates they issue

Certificate Validation

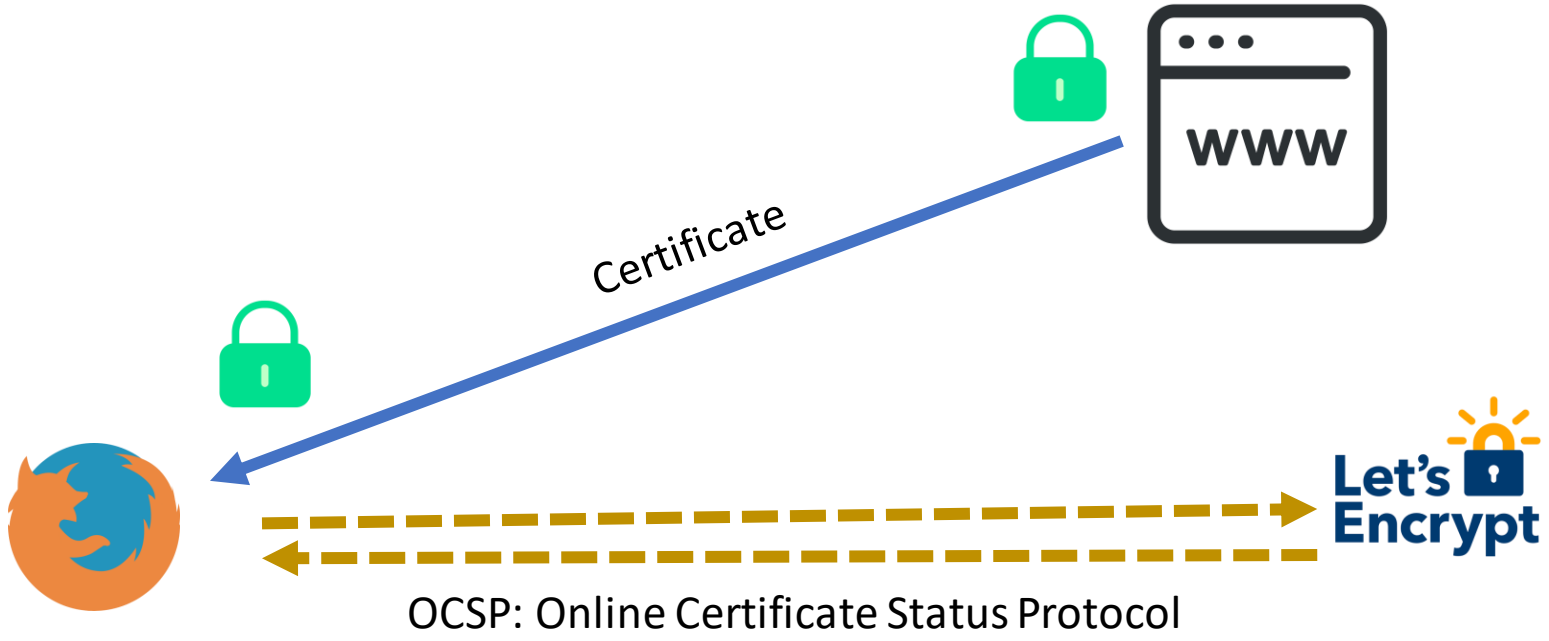
Certificate Authority is authorized to issue certificates

DNS CAA records

```
secosday.eu        0 issue "letsencrypt.org"              86400
secosday.eu        0 issuewild ";"                        86400
secosday.eu        0 iodef "mailto:ayesh@ayesh.me"        86400
```

Certificate Validation

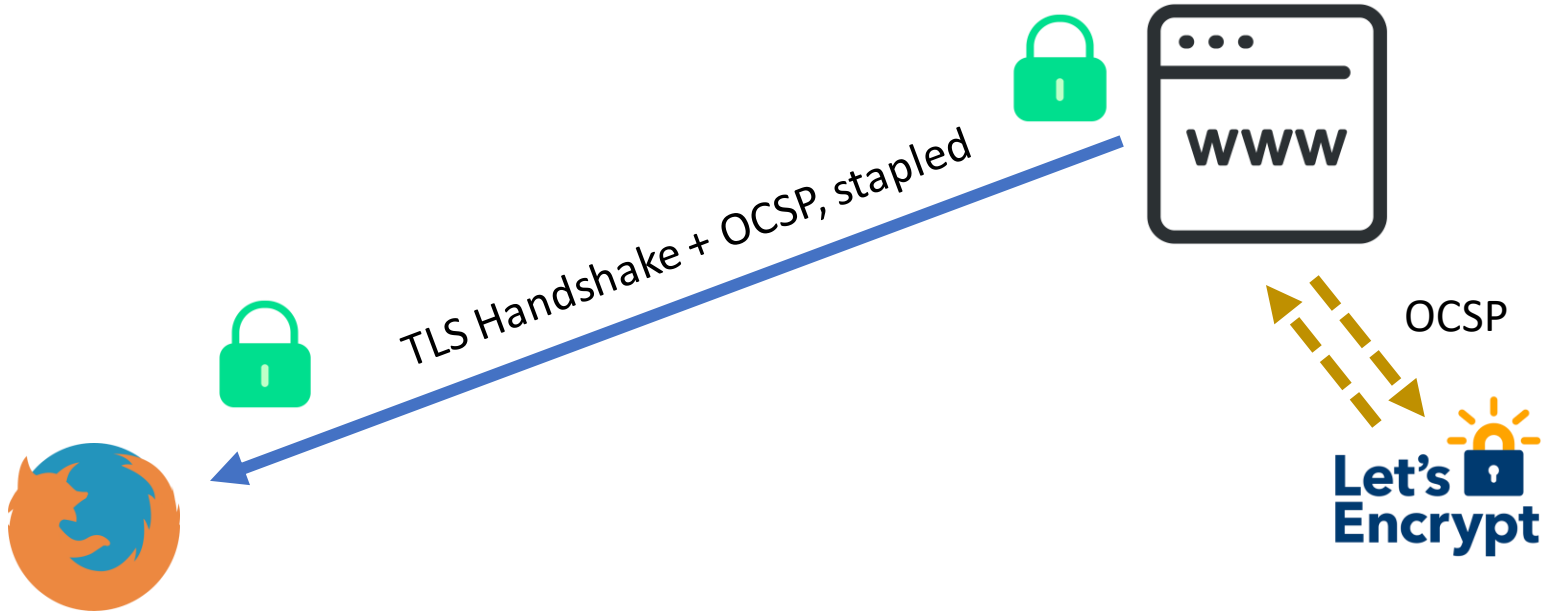
Certificate is valid and not revoked



- Additional network connection overhead
- Soft-fail by design, due to unreliable networking and CA servers

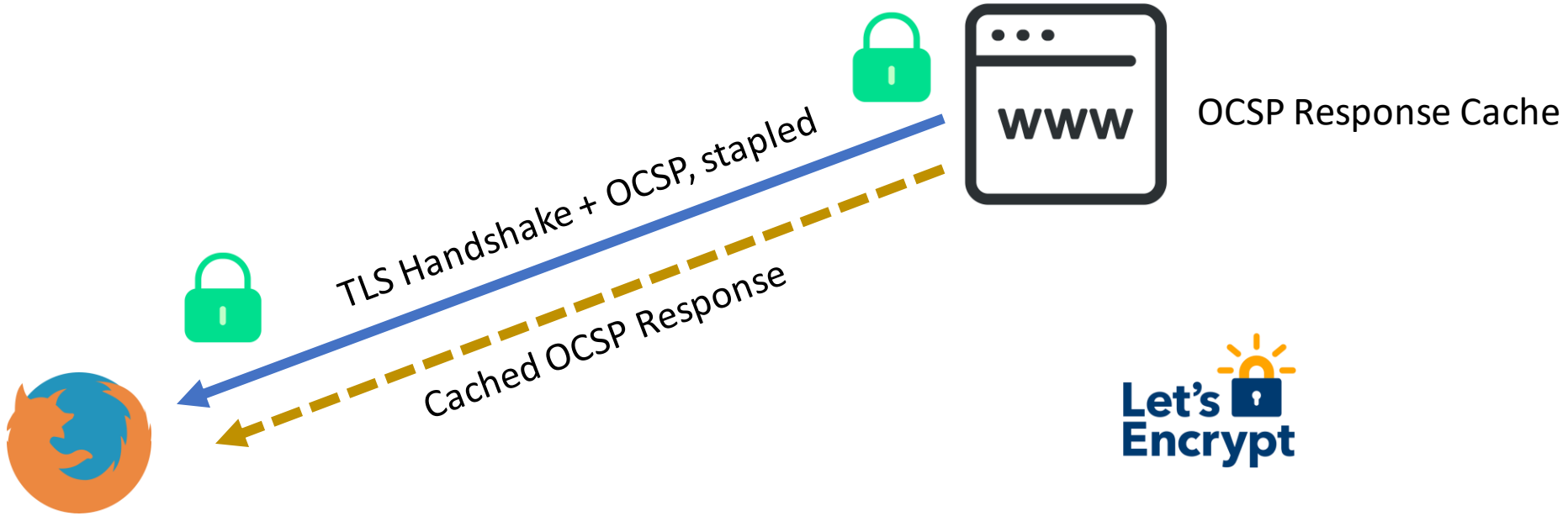
Certificate Validation

Certificate is valid and not revoked



Certificate Validation

Certificate is valid and not revoked



Certificate Validation

Certificate is valid and not revoked

This certificate authenticates
example.com, www.example.com

Valid from
15 Jan 2019 to 15 Apr 2019

Public key algorithm
prime256v1: 256 bits

Public key
…04 f1 a3 ff 46 e9 …
256 bits

Must-Staple

Certificate Validation

Certificate Authorities are accounted for the certificates they issue

A “trusted” certificate authority can issue a certificate for any domain name

There are over 200 “trusted” CA’s trusted in almost every system

We have no way to know if a CA issued a rogue certificate

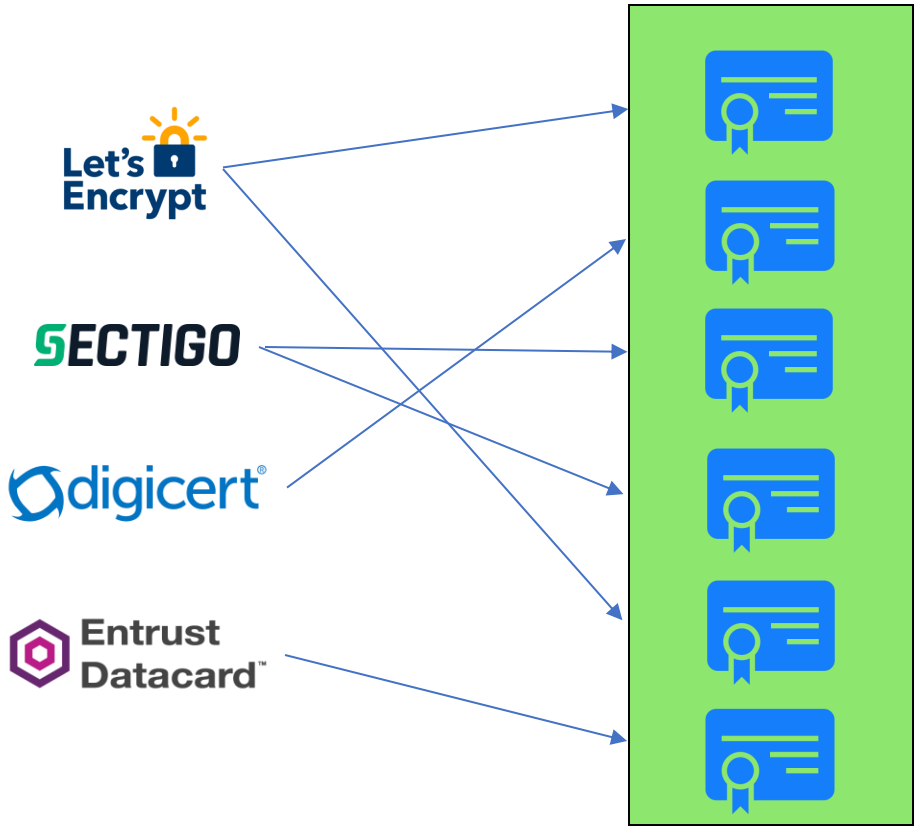
Certificate Validation

Certificate Authorities are accounted for the certificates they issue

Certificate Authority Wall of Shame

Certificate Validation

Certificate Authorities are accounted for the certificates they issue



+ Signed Certificate Timestamp

Append-only
Cannot remove items
Submit a pre-certificate and get Signed Certificate Timestamp

Validation

Transport Layer Security

Certificate Optimizations

- Use modern Elliptic Curve Cryptography certificates
- Serve RSA + ECC certificates

Encryption and Handshake Optimizations

- Do not use obsolete and old encryption and authentication mechanisms (RC4, 3DES, MD5, SHA1)
- Use mobile-friendly and fast encryption (CHACHA20-POLY1305, AES-GCM)
- Add TLS 1.3 support, DROP versions < 1.2

Certificate Validation

- DNS CAA records to indicate Certificate Authority Authorization
- Certificate Transparency, and SCT embedded in the certificate
- OCSP stapling and must-staple extension

Application Layer Security

An HTTP Request

```
GET /index.html
Host: example.com
Accept: text/html
```

```
HTTP 2.0 200 OK
Server: Apache
Content-Type: text/html
```


```
HTTP 2.0 200 OK
Server: Apache
Content-Type: text/html

Strict-Transport-Security: max-age=31536000;includeSubDomains;preload
x-Frame-Options: deny
X-Content-Type-Options: nosniff
Feature-Policy: accelerometer 'none';camera 'none’
Content-Security-Policy: default-src 'self'; script-src 'self’
Referrer-Policy: no-referrer
```

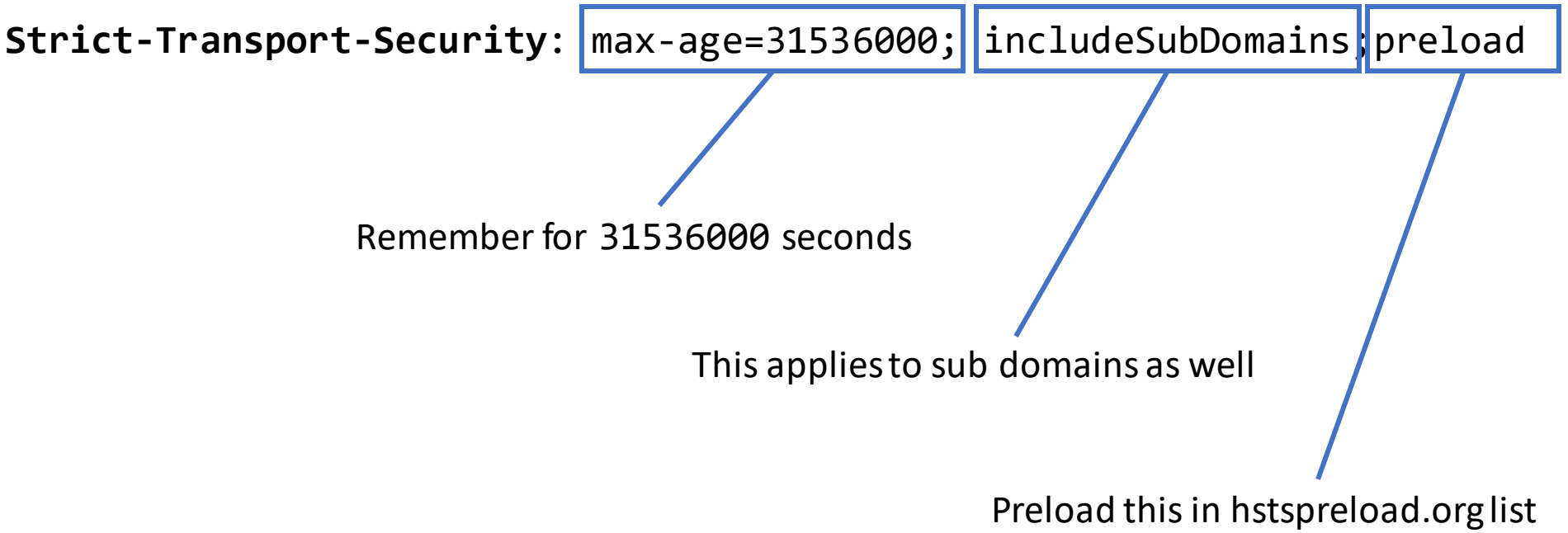
Set Custom Headers


```
Header always set name "value"
```


```
ddd_header name "value"
```

HTTP Strict-Transport-Security (HSTS)

Tells the browser to always connect over HTTPS (not plain HTTP), and remember this for a specified amount of time



Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security
https://hstspreload.org

X-Frame-Options

Can this page be embedded in an iframe

X-Frame-Options: deny

No other web page can embed this page in an iframe

X-Frame-Options: sameorigin

Only pages of same origin can embed this page in an iframe

Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options

X-Content-Type-Options

Do not sniff and try to guess the type of the content I’m about to send.

```
X-Content-Type-Options: nosniff
```

Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

Referrer-Policy

Control the HTTP Referrer header sent for page assets

```
Referrer-Policy: no-referrer
```

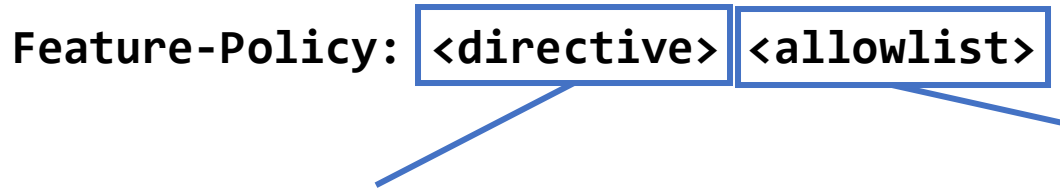
Do not send any header at all

```
Referrer-Policy: no-referrer
Referrer-Policy: no-referrer-when-downgrade
Referrer-Policy: origin
Referrer-Policy: origin-when-cross-origin
Referrer-Policy: same-origin
Referrer-Policy: strict-origin
Referrer-Policy: strict-origin-when-cross-origin
Referrer-Policy: unsafe-url
```

Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Feature-Policy

Allow or deny the usage of features in web page and child iframes



Feature that you want to control

- ambient-light-sensor
- autoplay
- accelerometer
- battery
- camera
- encrypted-media
- full-screen
- geolocation
- microphone
- payment
- picture-in-picture
- speaker
- sync-hxr
- webauthn

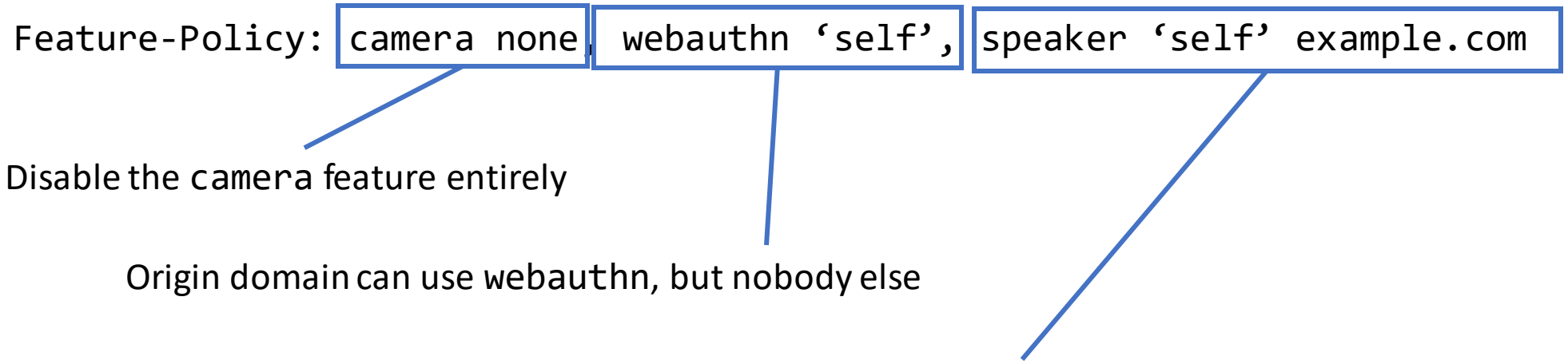
Deny, or white-list origins that can use the feature

- `*` : Allow all hosts
- `'none'` : Disable this feature
- `'self'` : Allow same origin URL only
- `example.com`: Allow example.com only.

Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Feature-Policy

Allow or deny the usage of features in web page and child iframes



Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Feature-Policy

Content-Security-Policy

Deny or whitelist which sources can the page contents can communicate with, connect to, and fetch resources from
Toggle or control certain types of security features

Content-Security-Policy: <directive> <allowlist>

Type of asset, or connection

Deny, or white-list origins that perform said connections

- `img-src`
- `media-src`
- `script-src`
- `style-src`
- `font-src`
- `form-actions`
- `navigate-to`
- …

- `block-all-mixed-content`
- `upgrade-insecure-requests`

- `*` : Allow all hosts
- `'none'` : Disable all connections
- `'self'` : Allow same origin URL only
- `example.com`: Allow example.com only.

Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Content-Security-Policy

Deny or whitelist which sources can the page contents can communicate with, connect to, and fetch resources from
Toggle or control certain types of security features

```
Content-Security-Policy: default-src 'self'; script-src 'self' cdn.example.com.com;
object-src 'self' i.visalogy.com; style-src 'self' i.visalogy.com; img-src 'self'
i.visalogy.com;
```

Use this rule for every connection type not mentioned here

Only allow scripts from origin URL and cdn.example.com only

Only allow images from origin URL

Reference: https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Content-Security-Policy

Further Resources

Further Resources

- https://www.ssllabs.com/ssltest/
- https://ssl-config.mozilla.org/
- https://cipherli.st/
- https://www.immuniweb.com/websec/
- https://www.immuniweb.com/ssl/

Questions?

No question is too small.

@Ayeshlive ayesh@ayesh.me

https://ayesh.me/talk/TLS-HTTP-Headers


THANK YOU
dziękuję
Ďakujem
tak
arigatô
paldies
mahalo
kop khun
děkuji
diolch
dankie
köszönöm
감사합니다
хвала
shukran
tänan
a dank
gràcies
ngiyabonga
Баярлалаа
dhanyavād
Дякую
Благодарам
ευχαριστώ
спасибо
благодаря
tack
grazie
Ǹh’gōi
Dank u
Благодаря ти
gracias
ස්තුතියි
mulţumesc
ačiū
תודה.
takk
nandri
danke
faleminderit
Xièxiè
choukrane
teşekkür ederim
obrigado
kiitos
Շնորհակալություն
terima kasih
hvala
grazzi

Perfectionist's Guide To

TLS Optimizations & HTTP Headers

Ayesh Karunaratne | https://ayesh.me/talk/TLS-HTTP-Headers