Web Server Design

Lecture 10 – HTTPS

Old Dominion University

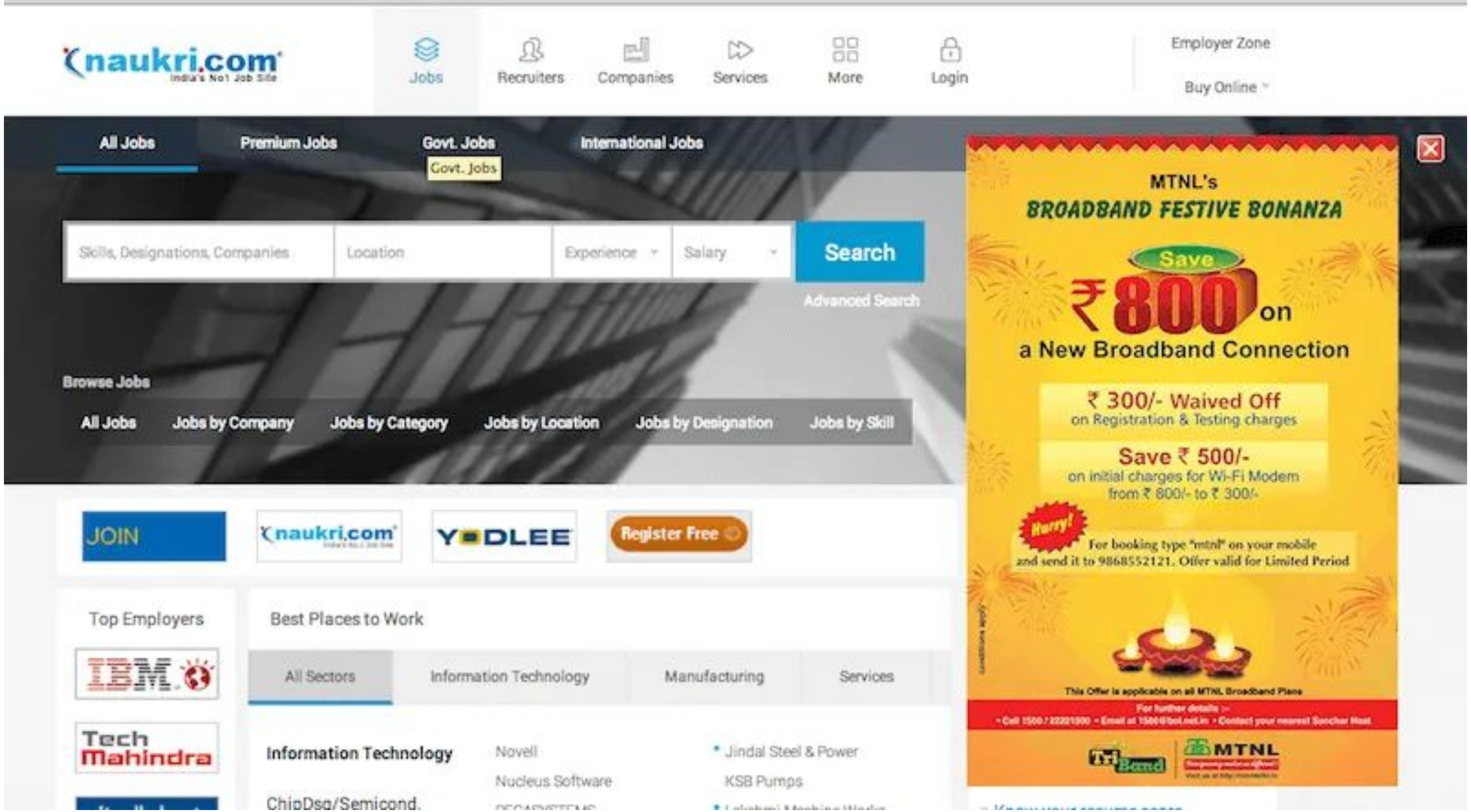
Department of Computer Science

CS 431/531 Fall 2019

Sawood Alam <salam@cs.odu.edu>

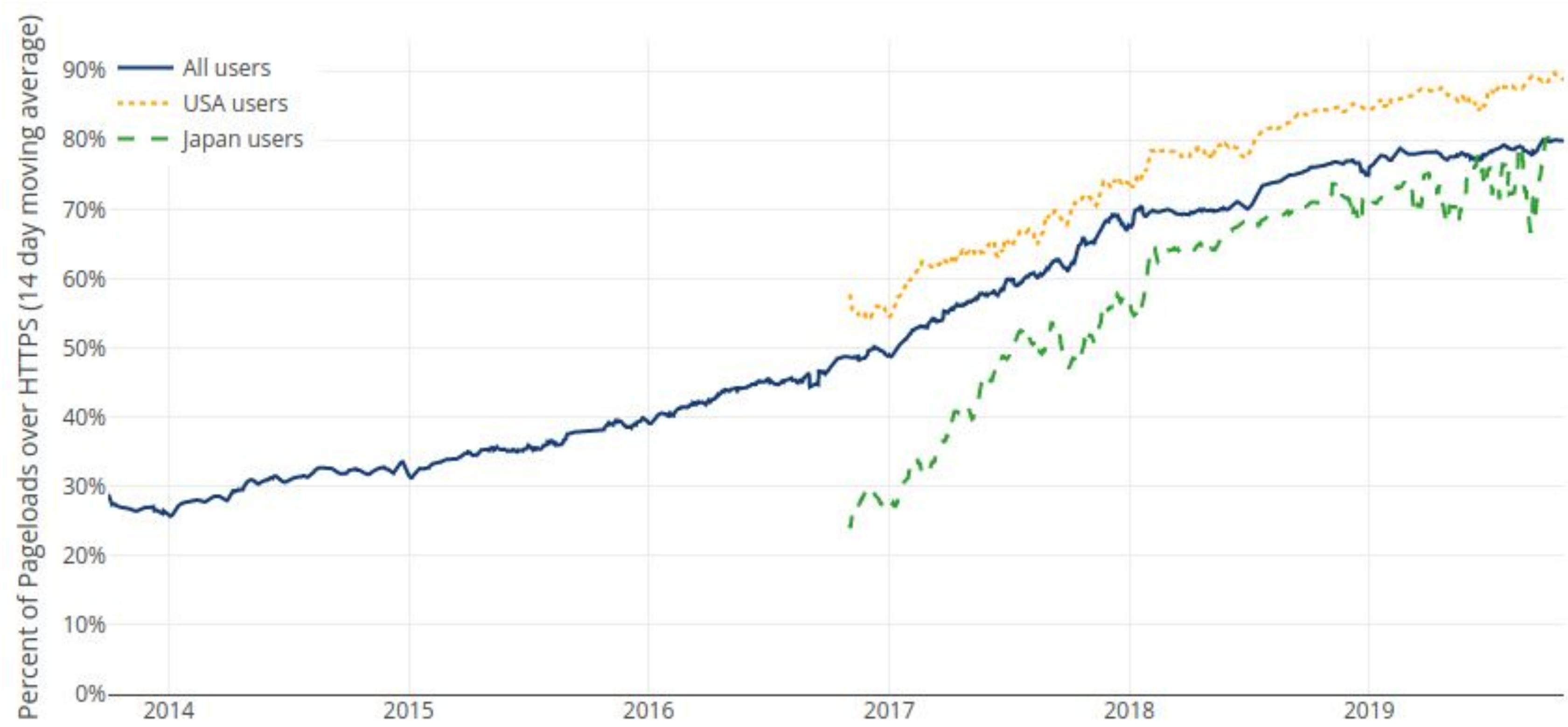
2019-10-31

ISPs Inject Ad In HTTP HTML Pages



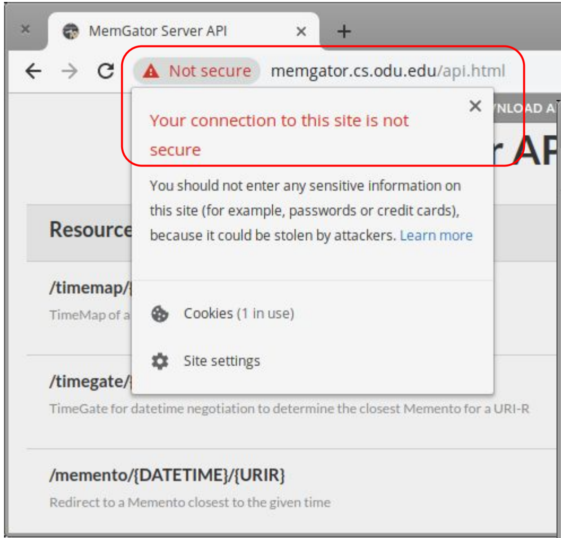
From: https://www.medianama.com/2015/06/223-mtnl-isp-advertising-airtel/

Percentage of Web Pages Loaded by Firefox Using HTTPS



From: https://letsencrypt.org/stats/

HTTP vs. HTTPS



Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers. Learn more

Cookies (1 in use)

Site settings

Resource

/timemap/

TimeMap of a

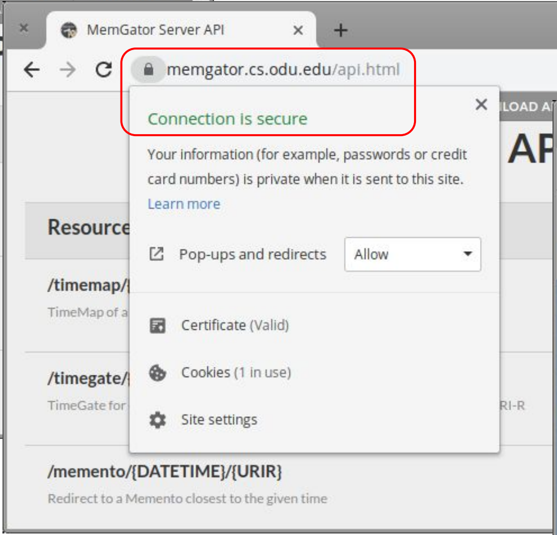
/timegate/

TimeGate for datetime negotiation to determine the closest Memento for a URI-R

/memento/{DATETIME}/{URIR}

Redirect to a Memento closest to the given time

No Certificate



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Pop-ups and redirects: Allow

Certificate (Valid)

Cookies (1 in use)

Site settings

Resource

/timemap/

TimeMap of a

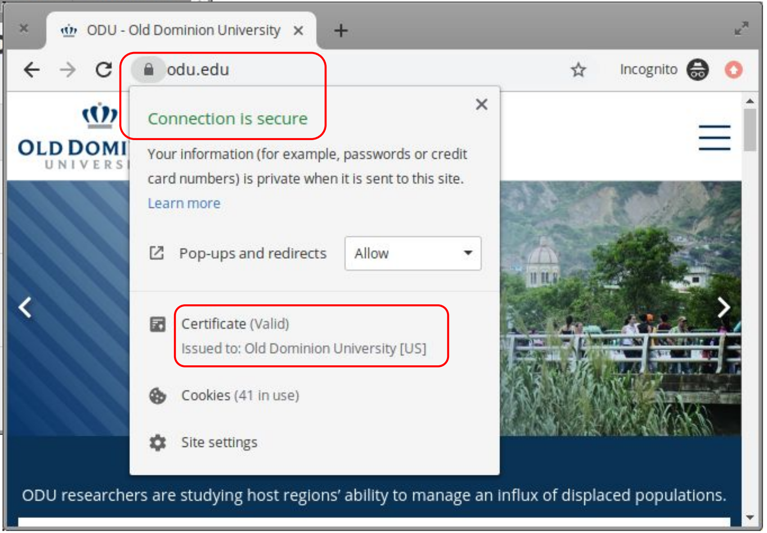
/timegate/

TimeGate for

/memento/{DATETIME}/{URIR}

Redirect to a Memento closest to the given time

Domain Validation



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Pop-ups and redirects: Allow

Certificate (Valid)
Issued to: Old Dominion University [US]

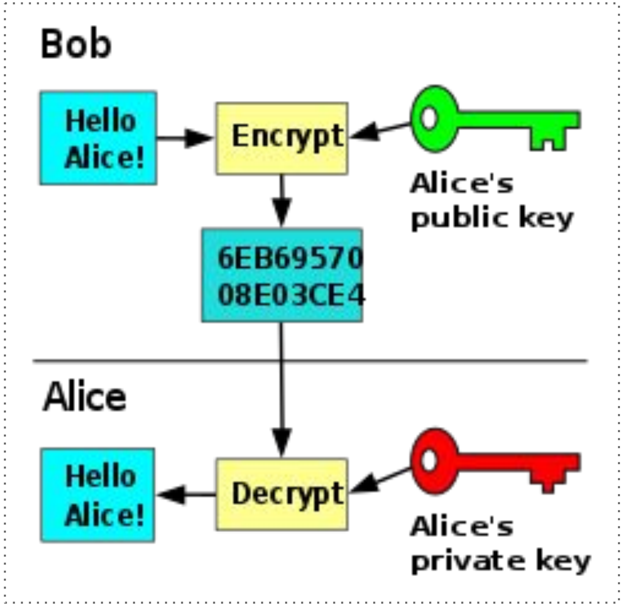
Cookies (41 in use)

Site settings

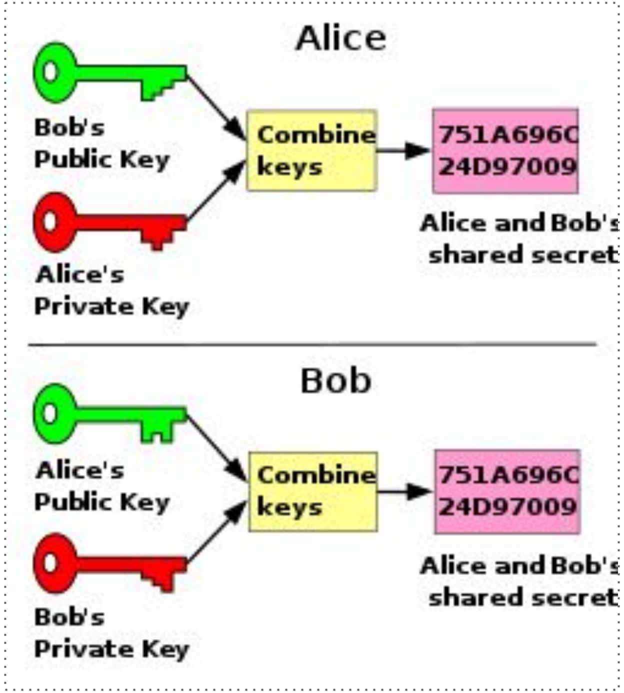
ODU researchers are studying host regions' ability to manage an influx of displaced populations.

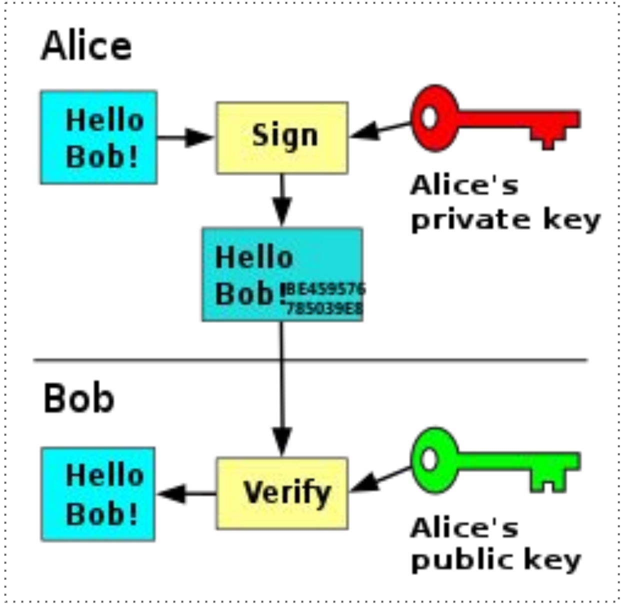
Organization/Extended Validation

Public-key Cryptography



Encryption



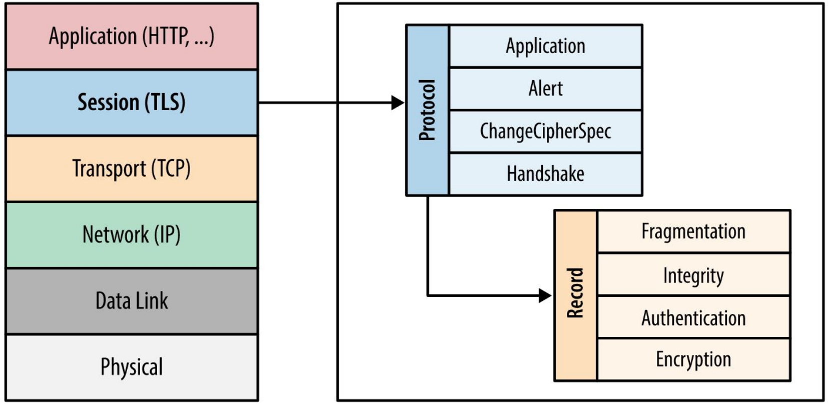


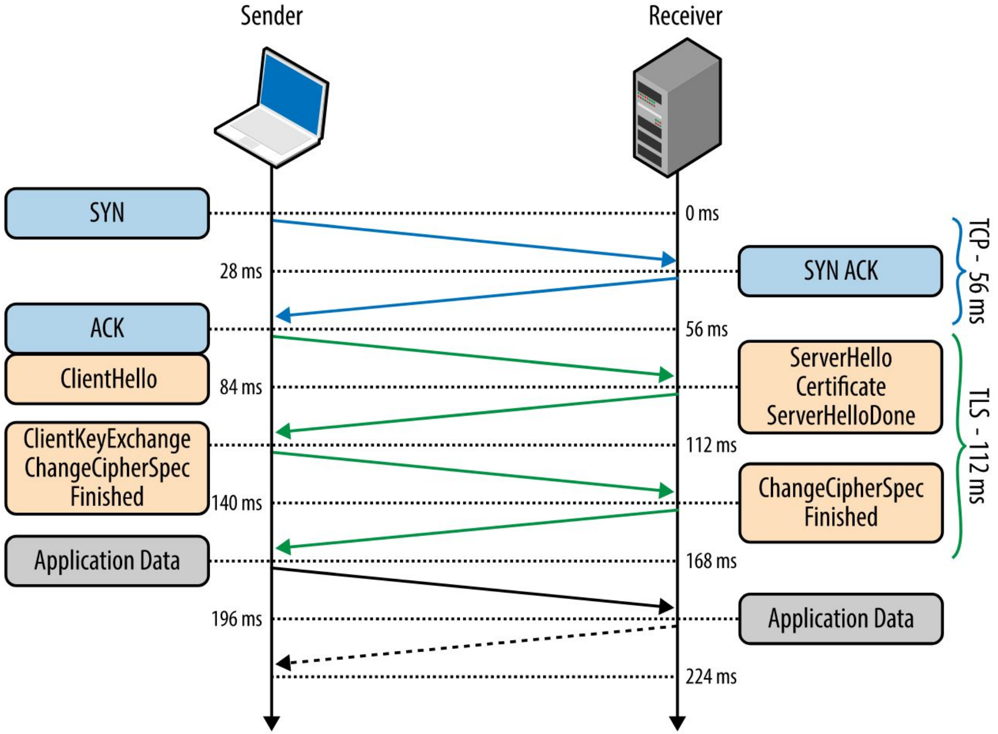
Signing

Diffie–Hellman key exchange

From: https://en.wikipedia.org/wiki/Public-key_cryptography

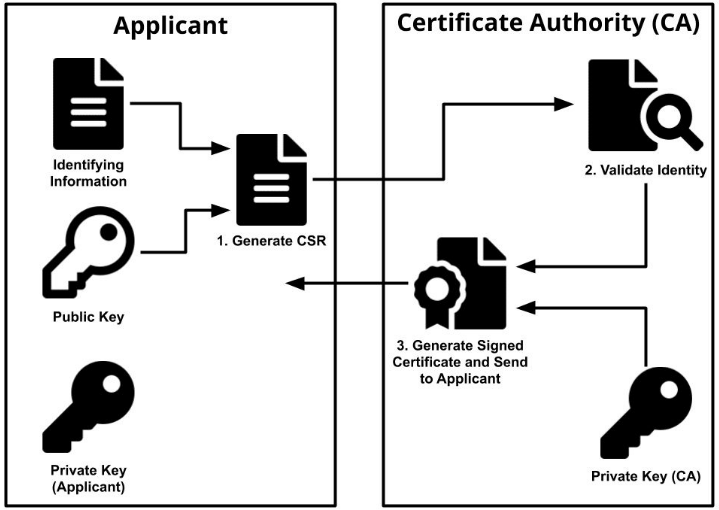
Transport Layer Security (TLS)





From: https://hpbn.co/transport-layer-security-tls/

Anatomy of TLS Certificate



Applicant

Identifying Information

Public Key

Private Key (Applicant)

1. Generate CSR

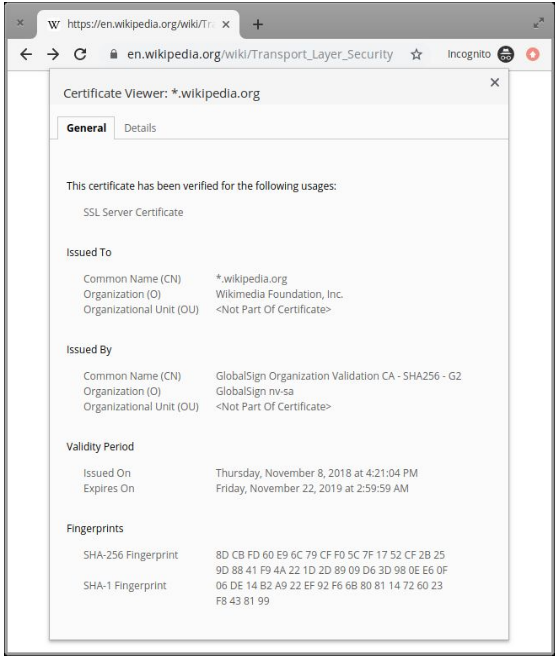
Certificate Authority (CA)

2. Validate Identity

3. Generate Signed Certificate and Send to Applicant

Private Key (CA)

Certificate Issuance from a Certificate Authority (CA)



https://en.wikipedia.org/wiki/Tr
en.wikipedia.org/wiki/Transport_Layer_Security
Incognito
General
Details

Certificate Viewer: *.wikipedia.org

This certificate has been verified for the following usages:

SSL Server Certificate

Issued To

Common Name (CN)	*.wikipedia.org
Organization (O)	Wikimedia Foundation, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

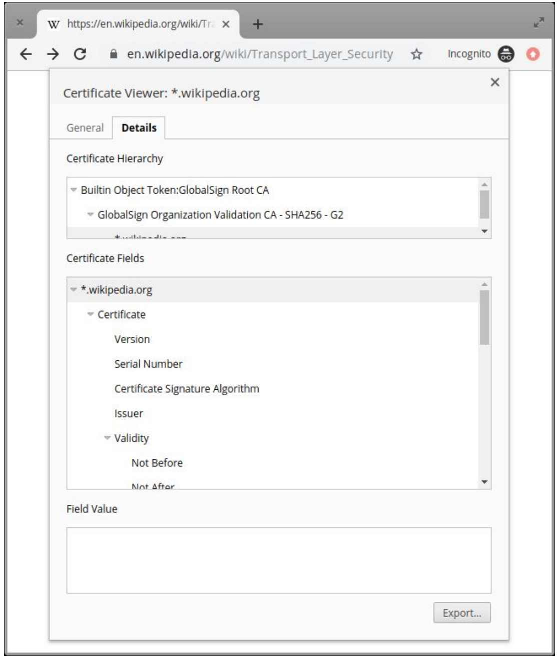
Common Name (CN)	GlobalSign Organization Validation CA - SHA256 - G2
Organization (O)	GlobalSign nv-sa
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Thursday, November 8, 2018 at 4:21:04 PM
Expires On	Friday, November 22, 2019 at 2:59:59 AM

Fingerprints

SHA-256 Fingerprint	8D CB FD 60 E9 6C 79 CF F0 5C 7F 17 52 CF 2B 25 9D 88 41 F9 4A 22 1D 2D 89 09 D6 3D 98 0E E6 0F
SHA-1 Fingerprint	06 DE 14 B2 A9 22 EF 92 F6 6B 80 81 14 72 60 23 F8 43 81 99



https://en.wikipedia.org/wiki/Tr
en.wikipedia.org/wiki/Transport_Layer_Security
Incognito
General
Details
Export...

Certificate Viewer: *.wikipedia.org

Certificate Hierarchy

- Builtin Object Token:GlobalSign Root CA
  - GlobalSign Organization Validation CA - SHA256 - G2
    - *.wikipedia.org

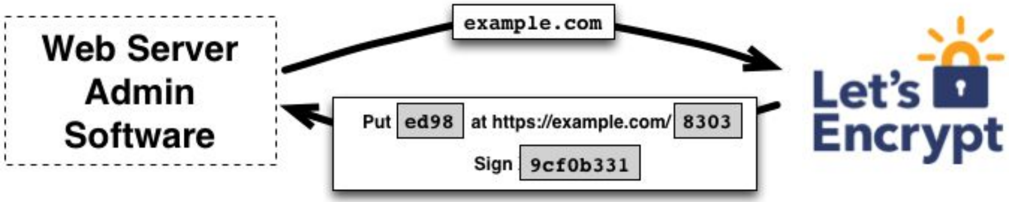
Certificate Fields

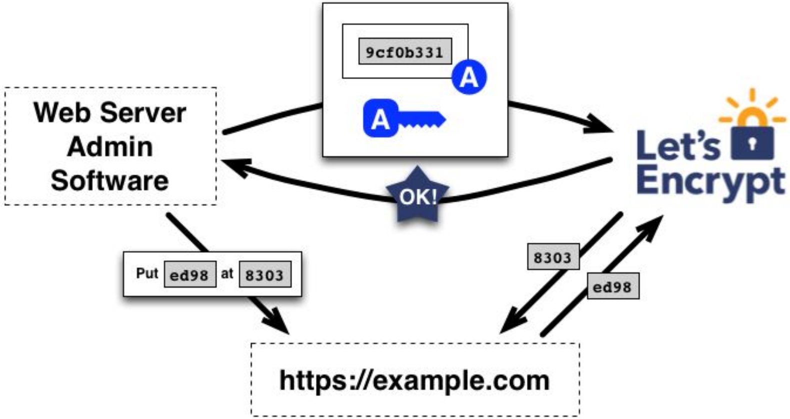
- *.wikipedia.org
  - Certificate
    - Version
    - Serial Number
    - Certificate Signature Algorithm
    - Issuer
    - Validity
      - Not Before
      - Not After

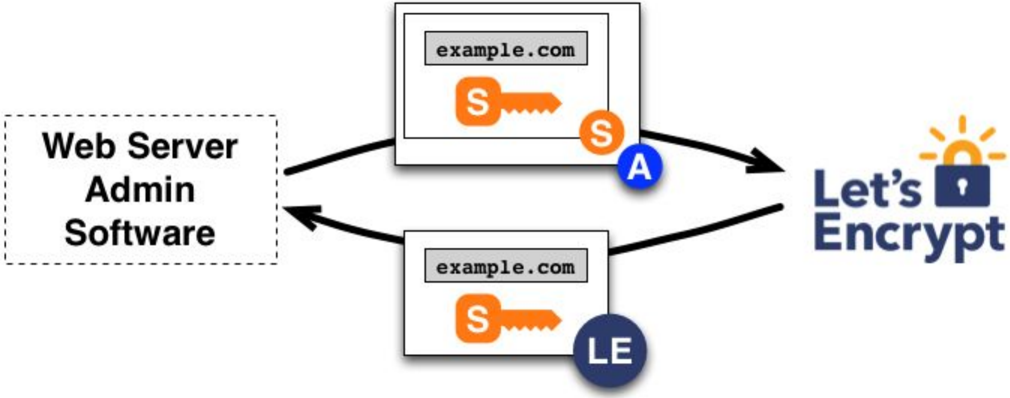
Field Value

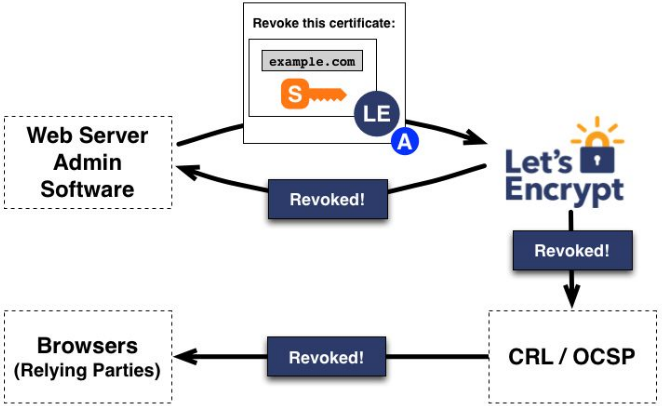
Certificate Viewer

Automatic Certificate Management Environment (ACME)


Web Server Admin Software
example.com
Put ed98 at https://example.com/ 8303
Sign 9cf0b331
Let's Encrypt







From: https://letsencrypt.org/how-it-works/

https://tools.ietf.org/html/rfc8555