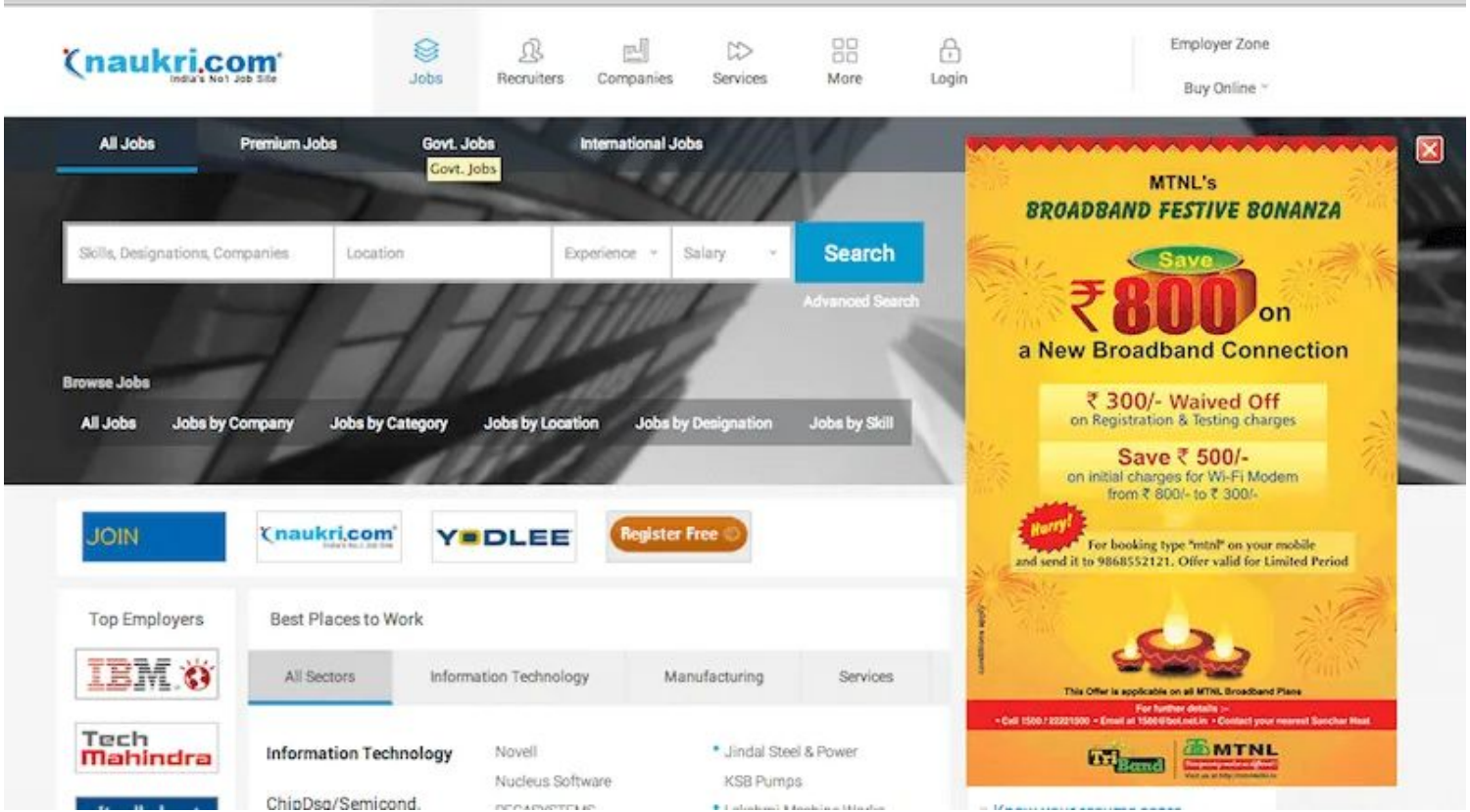
Web Server Design

Lecture 10 – HTTPS

Old Dominion University
Department of Computer Science
CS 431/531 Fall 2022
Sawood Alam <salam@cs.odu.edu>

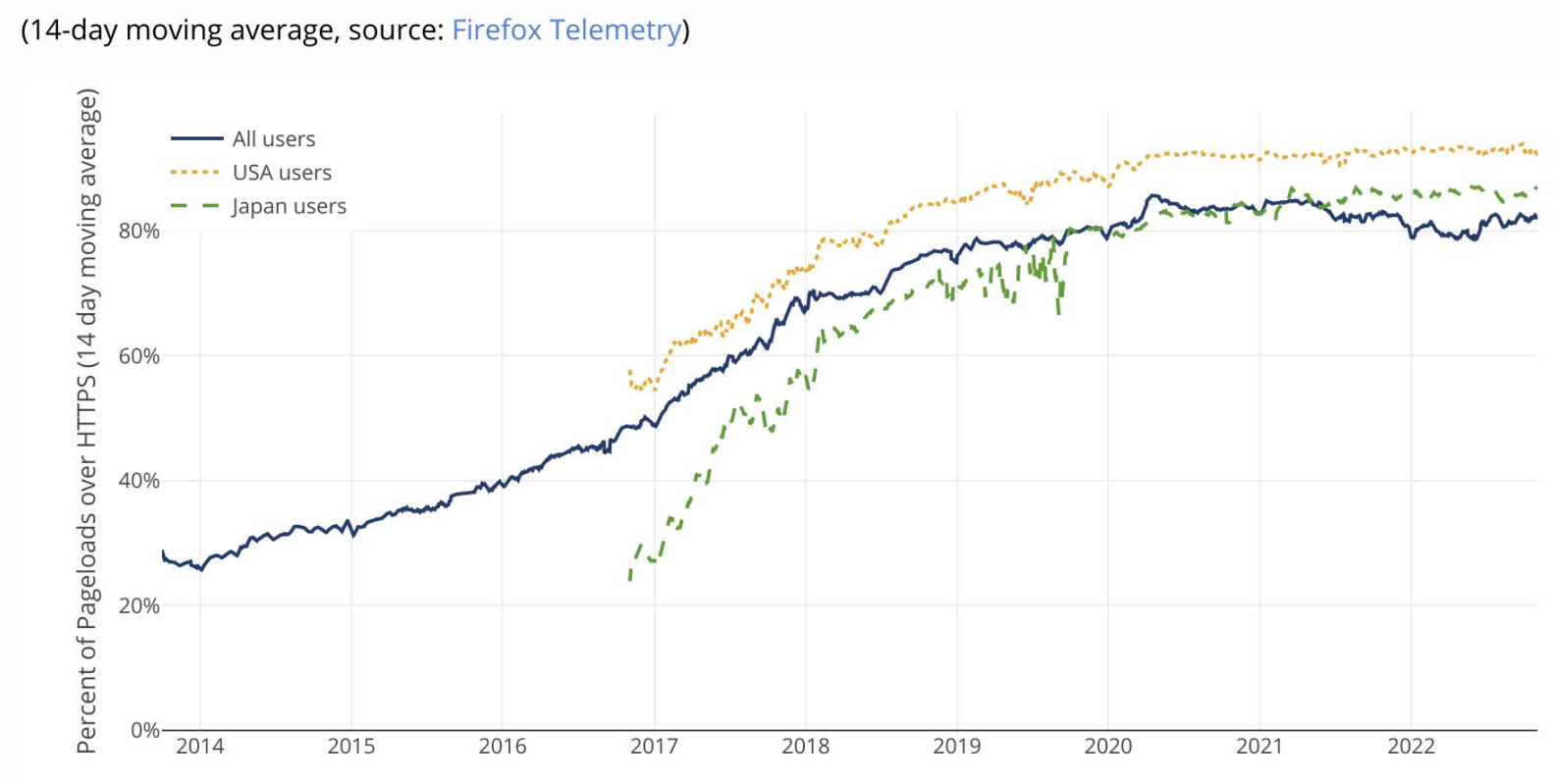
2022-11-02

ISPs Inject Ad In HTTP HTML Pages



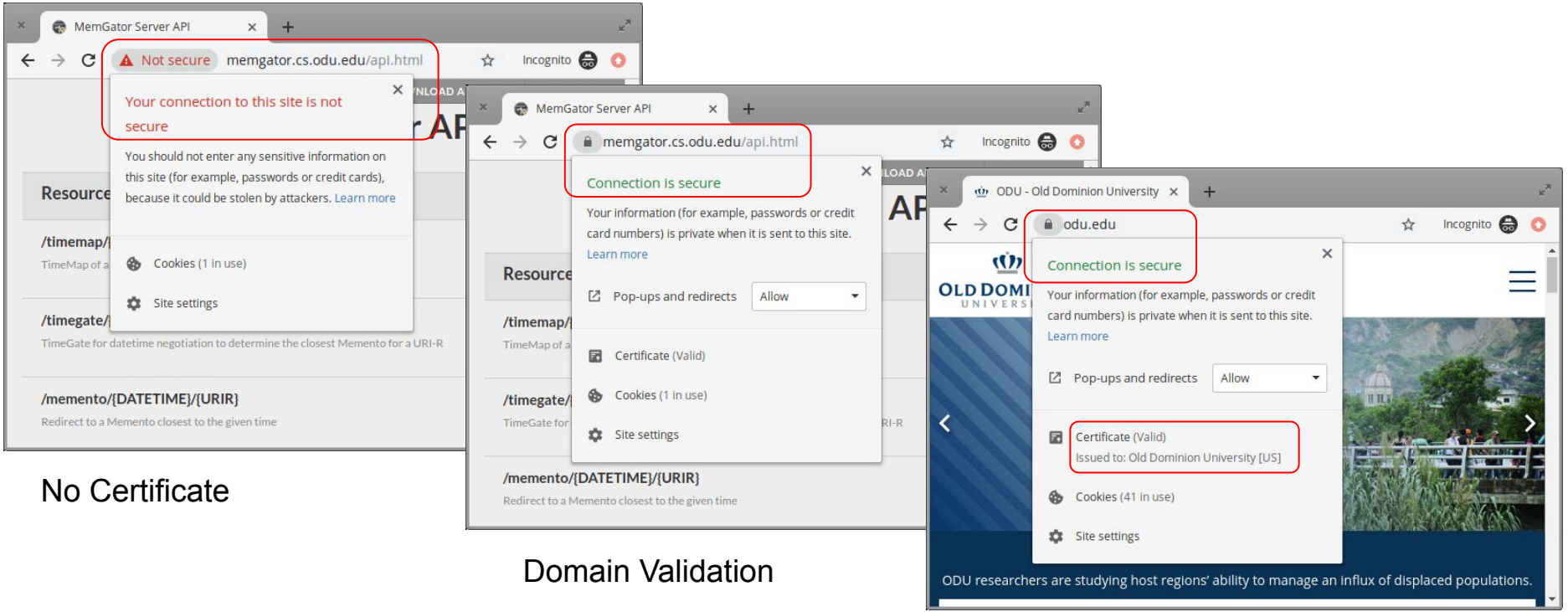
From: https://www.medianama.com/2015/06/223-mtnl-isp-advertising-airtel/

Percentage of Web Pages Loaded by Firefox Using HTTPS



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

HTTP vs. HTTPS

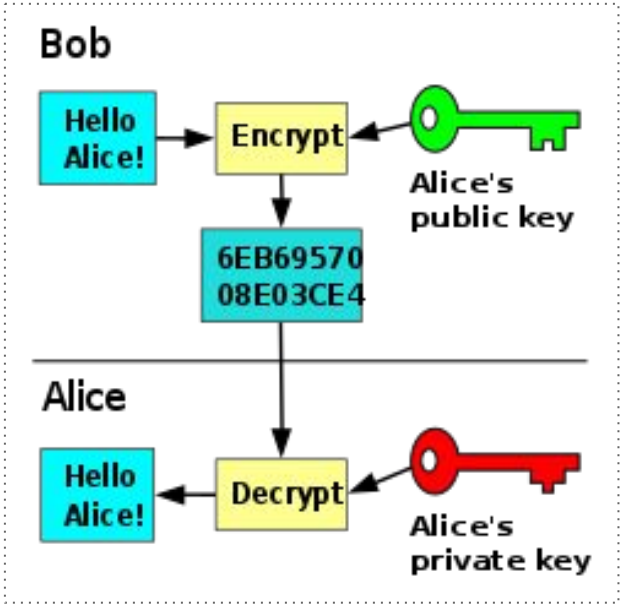


No Certificate

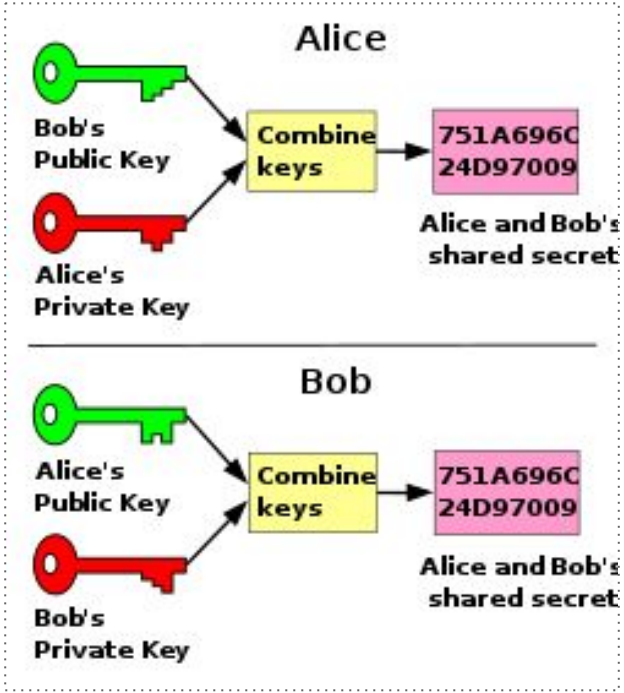
Domain Validation

Organization/Extended Validation

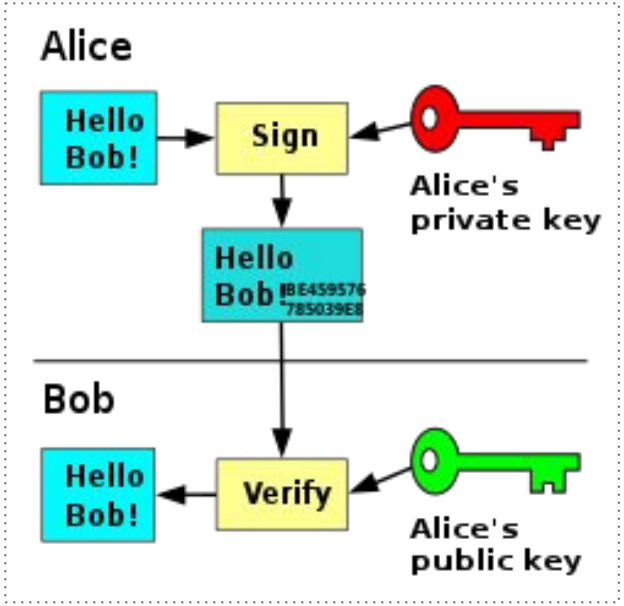
Public-key Cryptography



Encryption



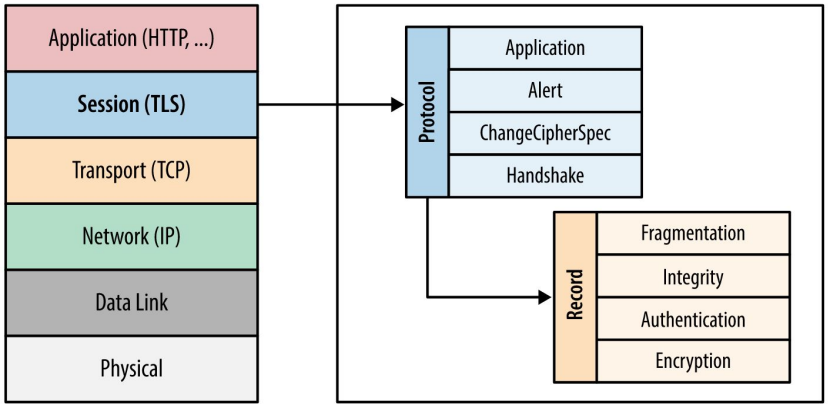
Diffie–Hellman key exchange



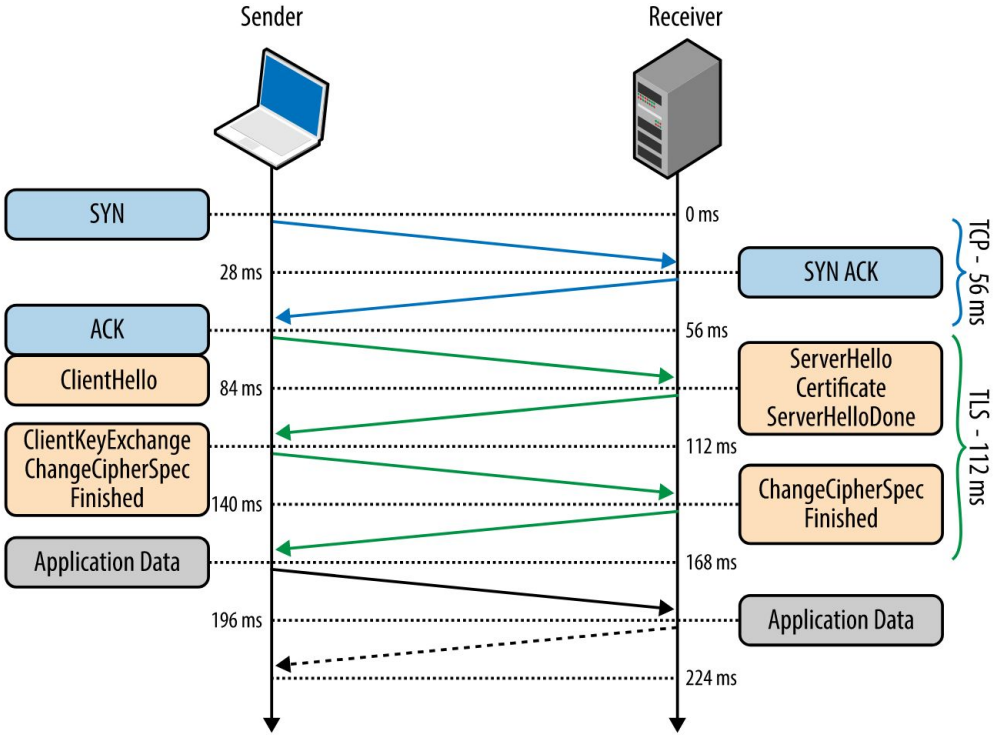
Signing

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

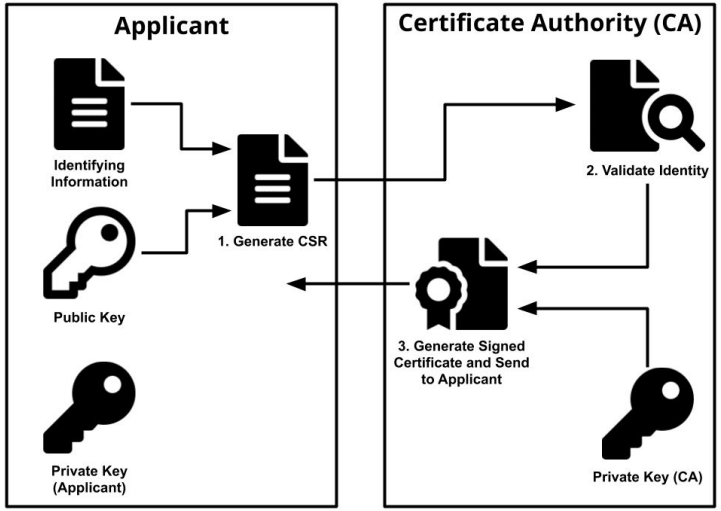
Transport Layer Security (TLS)



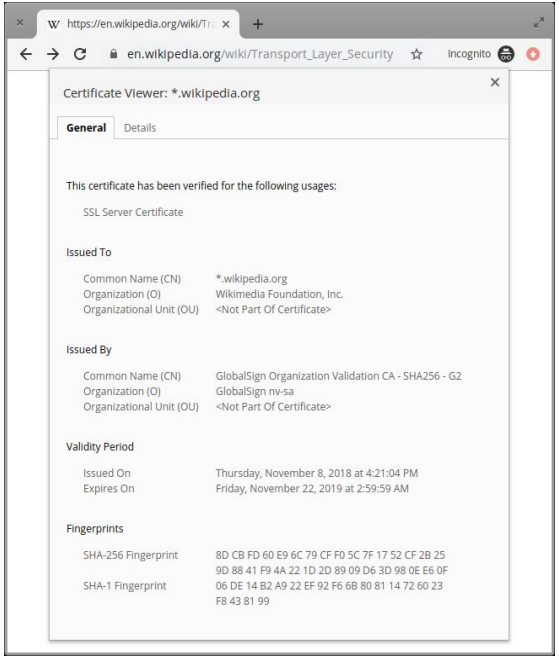
From: https://hpbn.co/transport-layer-security-tls/

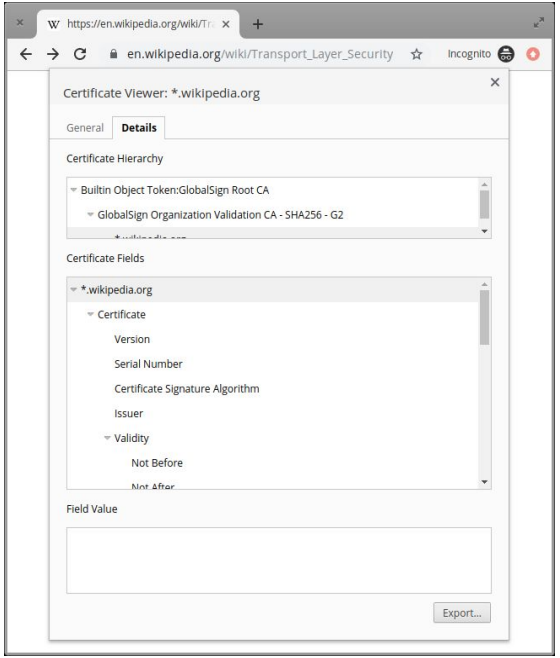


Anatomy of TLS Certificate



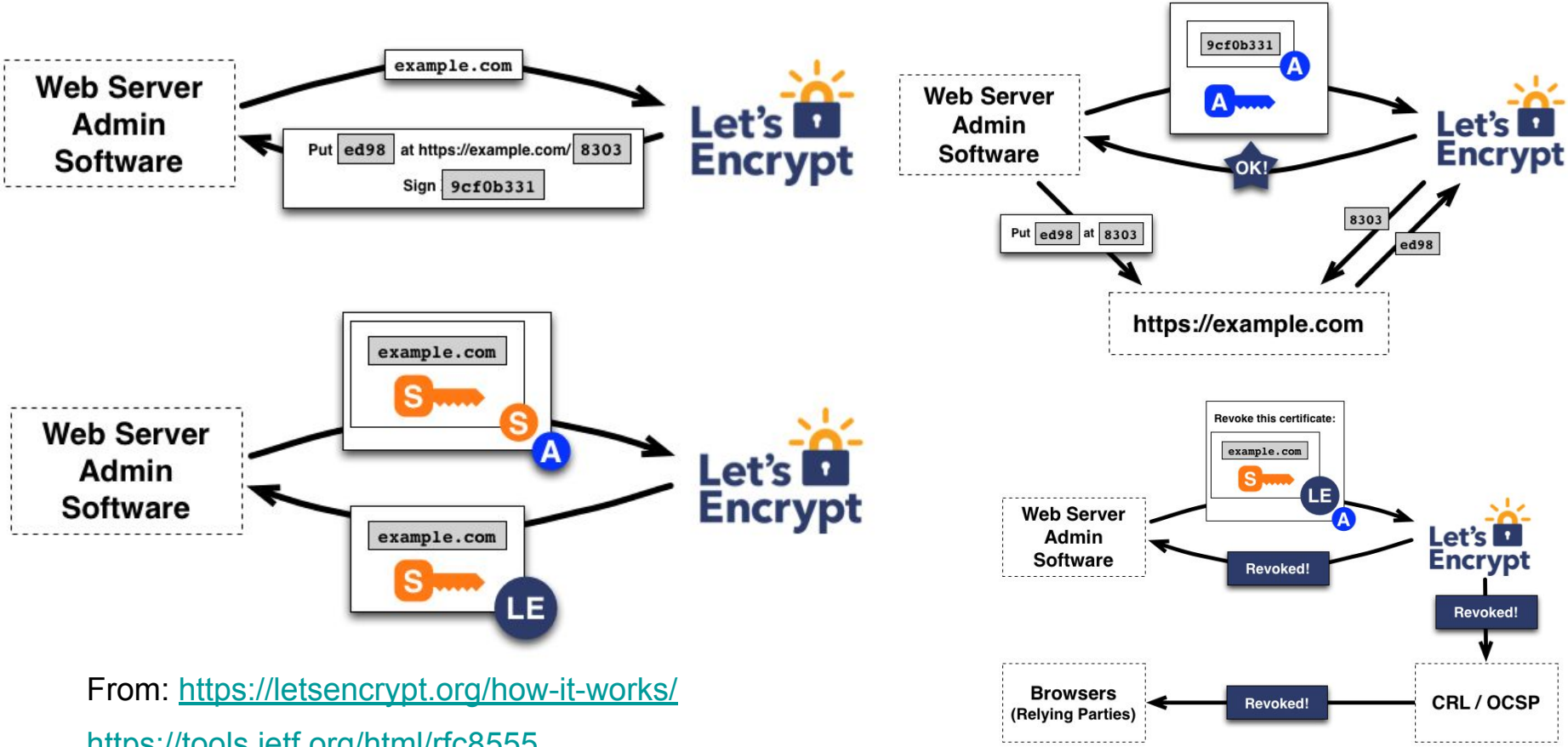
Certificate Issuance from a Certificate Authority (CA)





Certificate Viewer

Automatic Certificate Management Environment (ACME)



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

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