CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

PKI

Chris Samayoa

Week 15 – 1st Lecture
4/26/2022

Course Information

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

Objectives

- PKI
  - Asymmetric Encryption
  - Need for Trusted Authorities
  - Digital Certificates
  - Certificate Authorities
  - Chain of Trust

PKI

- Public Key Infrastructure (PKI)
  - Framework for encrypting communications between two nodes
    - Server-to-server
    - Client-to-client
    - Server-to-client
  - Most common form uses private and public key combination (asymmetric)
    - Allows for encrypted messaging
    - Allows for digital signatures to verify authenticity
  - PKI Certificates verify the owner (authentication) of a private key to allow for a trusted relationship
- Why use PKI?
  - Authentication
    - Signatures
  - Encryption
  - Data integrity
    - e.g. signed applications

Objectives

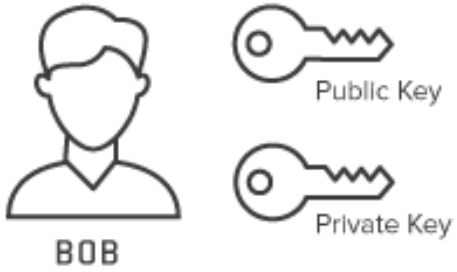
CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- PKI
  - Asymmetric Encryption
  - Need for Trusted Authorities
  - Digital Certificates
  - Certificate Authorities
  - Chain of Trust

Asymmetric Encryption

- Public key can be used by anyone to encrypt data
- Private key can be used by specific entity to decrypt data
- Common uses?
  - SSH algorithms
  - SSL/TLS
  - S/MIME encrypted email
  - Code signing
  - Bitcoin/Blockchain
  - Signal private messenger
  - Digital signatures
  - Authenticating nodes connecting to a wireless network
  - Authenticating connections to your VPN
  - Smart card authentication
- Powers PKI

PKI (cont'd)



Decrypt: $D(K_{priv}C) = M$

Sign: $S = E(K_{priv}M)$

Encrypt: $C = E(K_{pub}M)$

Verify: $D(K_{pub}S) = M$

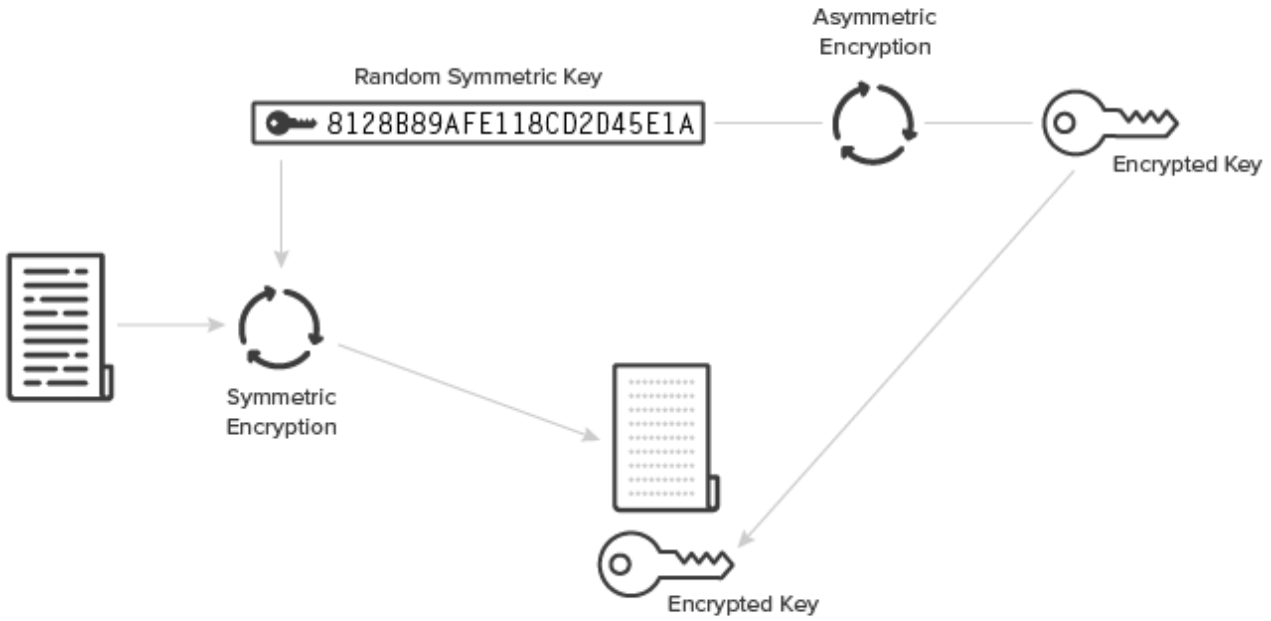
RSA, Diffie-Hellman, ECC

- SSH
- SSL / TLS
- S/MIME encrypted email
- Code Signing
- Bitcoin / Blockchain
- Signal Private Messenger
- Public Key Infrastructure

Source: https://www.keyfactor.com/resources/what-is-pki/

PKI (cont'd)

- Symmetric encryption is faster than asymmetric encryption
  - Asymmetric is often used just to send a symmetric key instead of a whole message



Source: https://www.keyfactor.com/resources/what-is-pki/

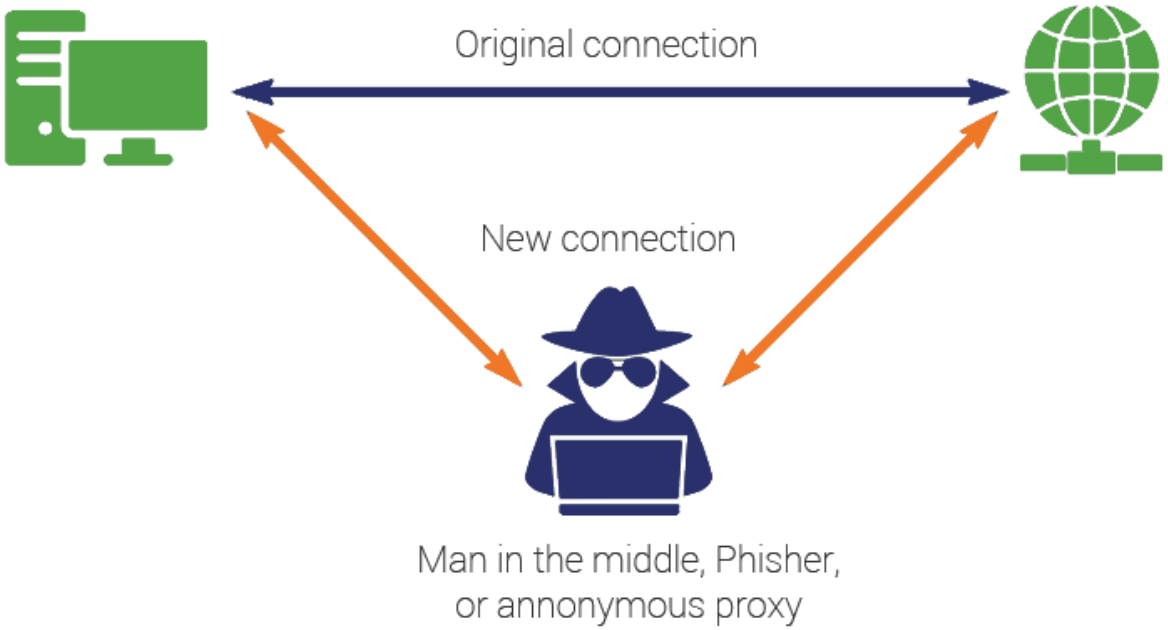
Objectives

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- PKI
  - Asymmetric Encryption
  - Need for Trusted Authorities
  - Digital Certificates
  - Certificate Authorities
  - Chain of Trust

PKI Problem

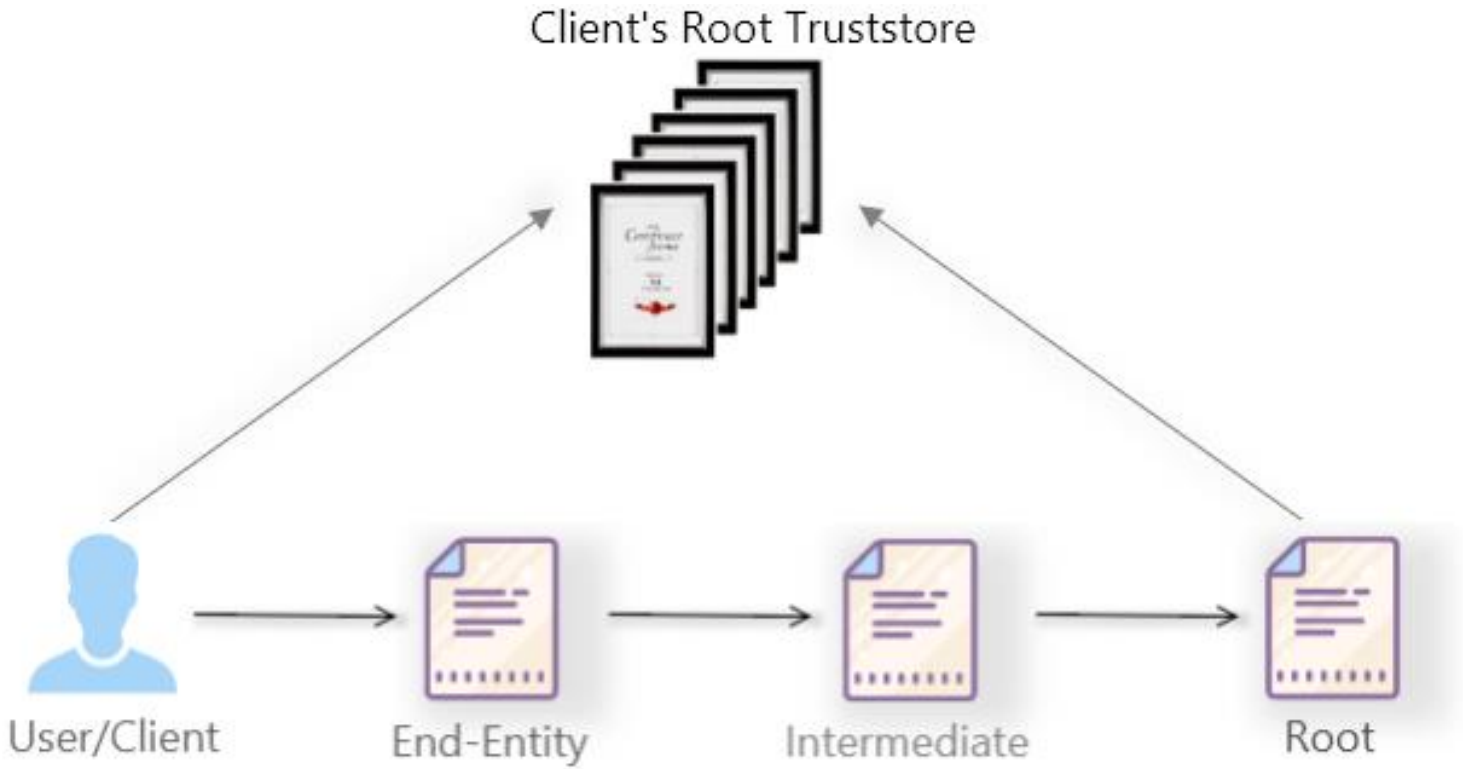
- How do you know that the public key you received comes from the entity you are trying to communicate with?
  - Major potential for MitM attack



Source: https://www.thesslstore.com/blog/man-in-the-middle-attack-2/

PKI Solution

- Trusted third party



Source: https://www.keyfactor.com/blog/certificate-chain-of-trust/

Objectives

- PKI
  - Asymmetric Encryption
  - Need for Trusted Authorities
  - Digital Certificates
  - Certificate Authorities
  - Chain of Trust

Digital Certificates

- Verify the identify of a device or user and enable encrypted connections
  - aka X.509 certificates or PKI certificates
    - IETF – RFC 5280
    - https://datatracker.ietf.org/doc/html/rfc5280
- Features
  - Mechanism for authentication
  - Hold information about a particular entity
  - Issued by trusted third party
  - Tamper-resistant
  - Authenticity of document can be proved
  - Trackable back to issuer
  - Set expiration date
  - Is presented for validation
  - Authenticating connections to your VPN
  - Smart card authentication

Digital Certificates (cont'd)

- Major Components
  - Digital Certificates
    - Electronic identification for websites and organizations
    - Can be self-created or obtained through a trusted third-party issuer
  - Certificate Authority (CA)
    - Vet organizations requesting certificates
    - Issue certificates
    - Establish "trusted" relationships
  - Certificate Revocation Lists (CRLs)
    - Mechanism to track revoked certificates

Objectives

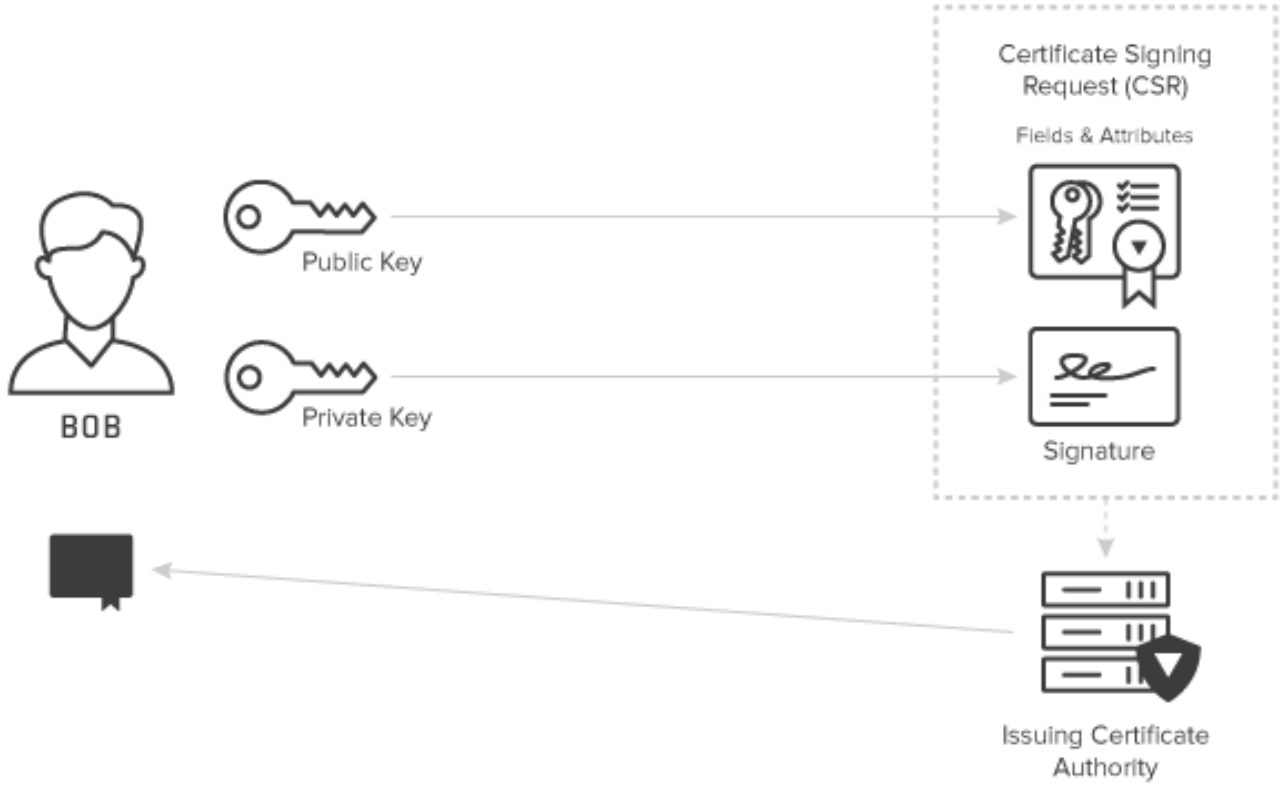
- PKI
  - Asymmetric Encryption
  - Need for Trusted Authorities
  - Digital Certificates
  - Certificate Authorities
  - Chain of Trust

Certificate Authority

- Overview
  - Responsible for creating and issuing digital certificates, including
    - Vetting methods for certificate requestors
    - Scope of certificate(s)
    - Parameters specified within certificate(s)
- Certificate creation process
  - Private key generated and used to compute corresponding public key
  - CA requests identifying attributes of the private key owner and vets the information
  - Public key and vetted attributed are encoded into a Certificate Signing Request (CSR)
  - CSR is signed by key owner to prove possession of specific private key
  - Issuing CA validates the request and signs the certificate with the CA's own private key
    - Note that each CA also has its own public and private keys
    - Establishes need for CA hierarchies
- As long as CA is deemed trustworthy by end users, they can be used to verify the owner of a particular public key

Source: https://www.keyfactor.com/resources/what-is-pki/

Certificate Authority (cont'd)



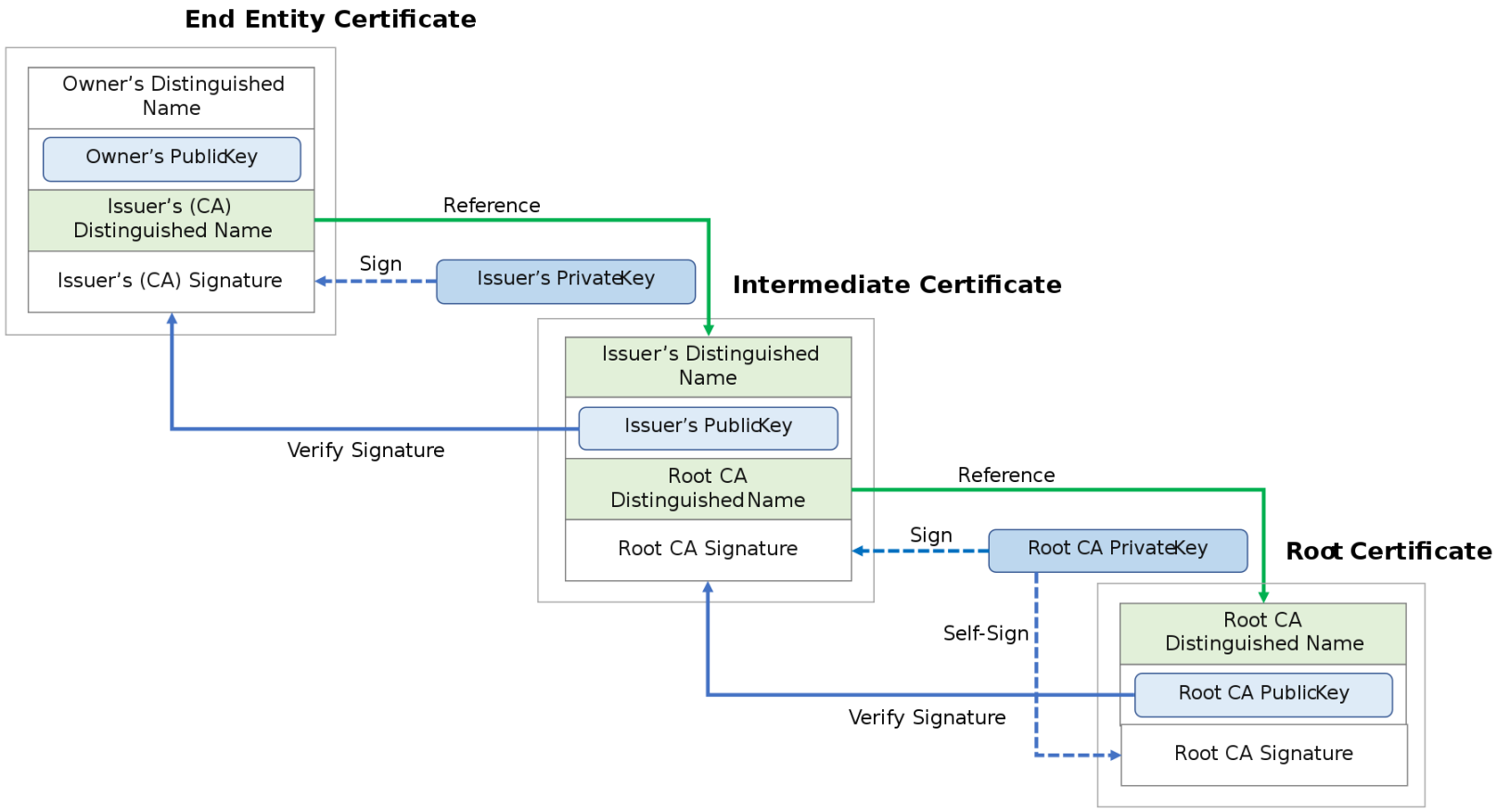
Source: https://www.keyfactor.com/resources/what-is-pki/

Objectives

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- PKI
  - Asymmetric Encryption
  - Need for Trusted Authorities
  - Digital Certificates
  - Certificate Authorities
  - Chain of Trust

PKI Chain of Trust



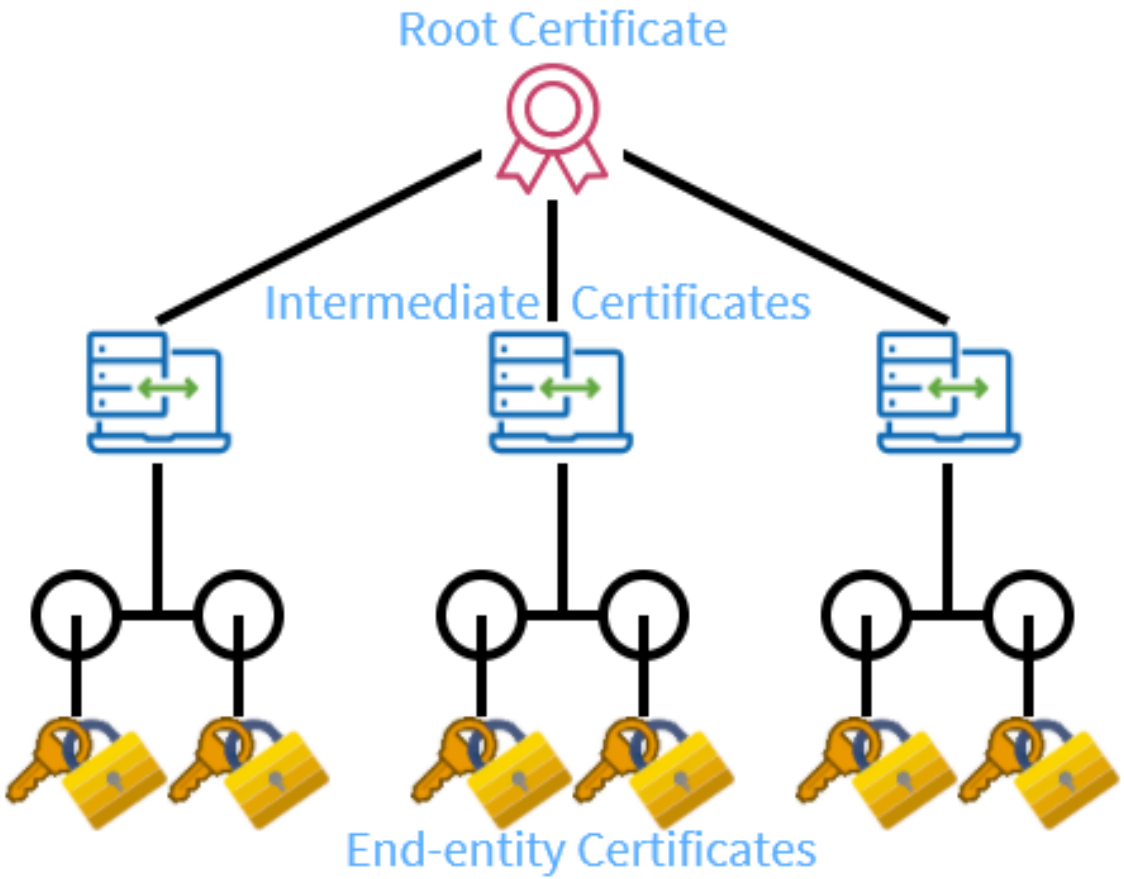
Source: https://en.wikipedia.org/wiki/Chain_of_trust#/media/File:Chain_Of_Trust.svg

Chain of Trust

- Types of entities
  - Root CA
    - Self-signed certificate -> “trust anchor”
    - Must be trusted for entire process to work
    - Very closely guarded – often kept “offline”
    - Expire every 15-20 years
  - Intermediate CA
    - Responsible for issuing certificates
      - To other intermediate CAs
      - To end-entity
    - Provides extra level of security between end-entity servers and root CA
  - End-entity Certificate
    - Does not guarantee that subject is trustworthy
    - Certificates are typically issued for organizations (not employees)
    - Parameters specified within certificate(s)

Source: https://www.keyfactor.com/blog/certificate-chain-of-trust/

Typical Trust Model



Source: https://www.keyfactor.com/blog/certificate-chain-of-trust/

Digital Certificate Risks

- What happens if private keys are compromised?
  - End-entity
    - Communication to that server can no longer be authenticated
    - Certificate needs to be revoked
    - New certificate needs to be issued
  - Intermediate CA
    - All end-entity certificates issued by the CA must be revoked and reissued
    - New asymmetric keys
    - New certificate must be issued by root CA (or other authority)
  - Root CA
    - All child CA certificates and end-entity certificates issued by those child CAs must be reissued
    - Root CA must be re-established

Certificate Revocation Lists

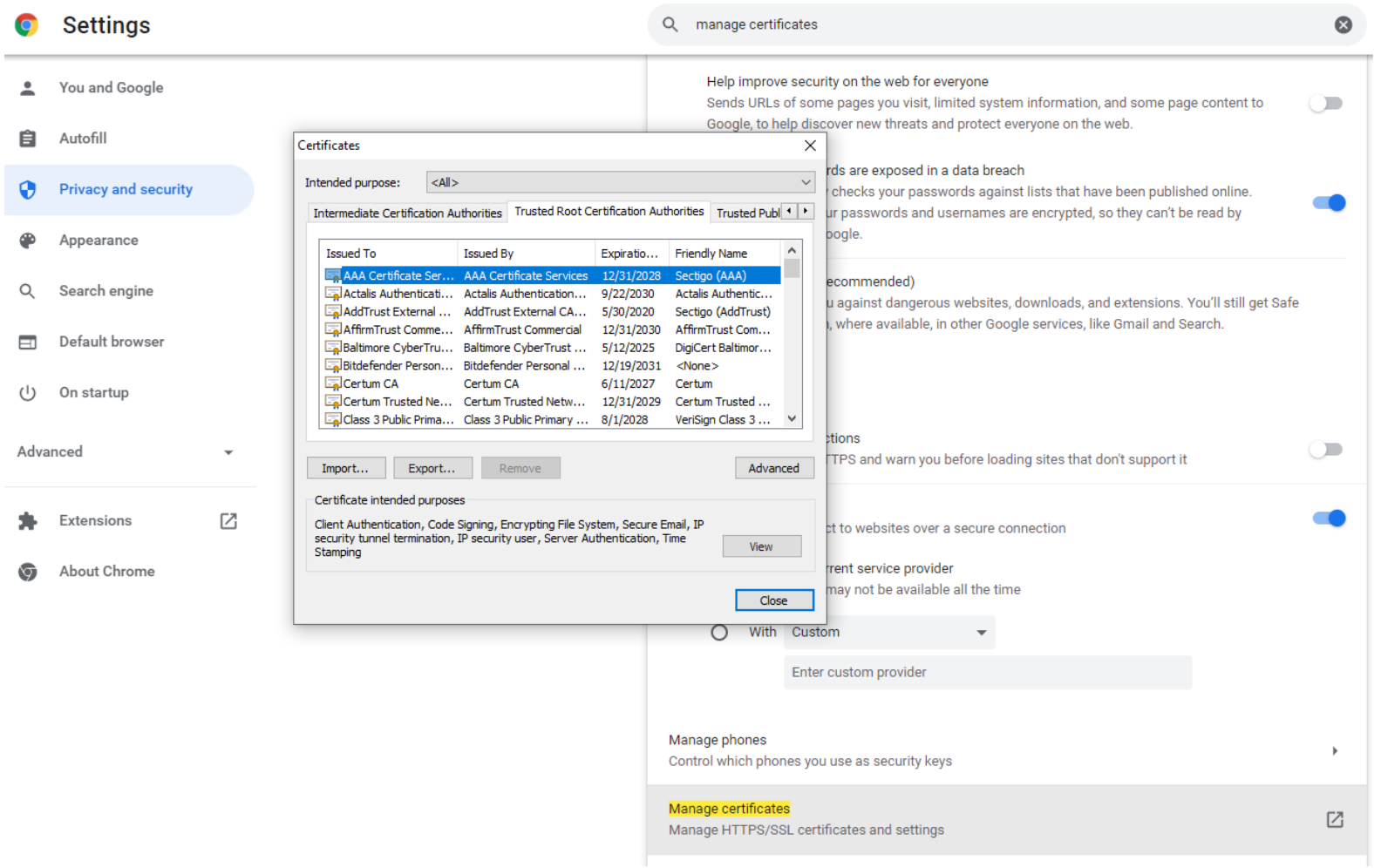
- Each CA must issue its own certificate revocation lists
  - Part of the standard for X.509 certificates
- Consumers must check CRLs for them to be effective
  - Slows down authentication process
    - Slower for each part of the hierarchy checked
- Were not commonly used before
- Have grown in usage by consumers
  - Due to internet security concerns

Check CRL

Source: https://www.thesslstore.com/blog/crl-explained-what-is-a-certificate-revocation-list/

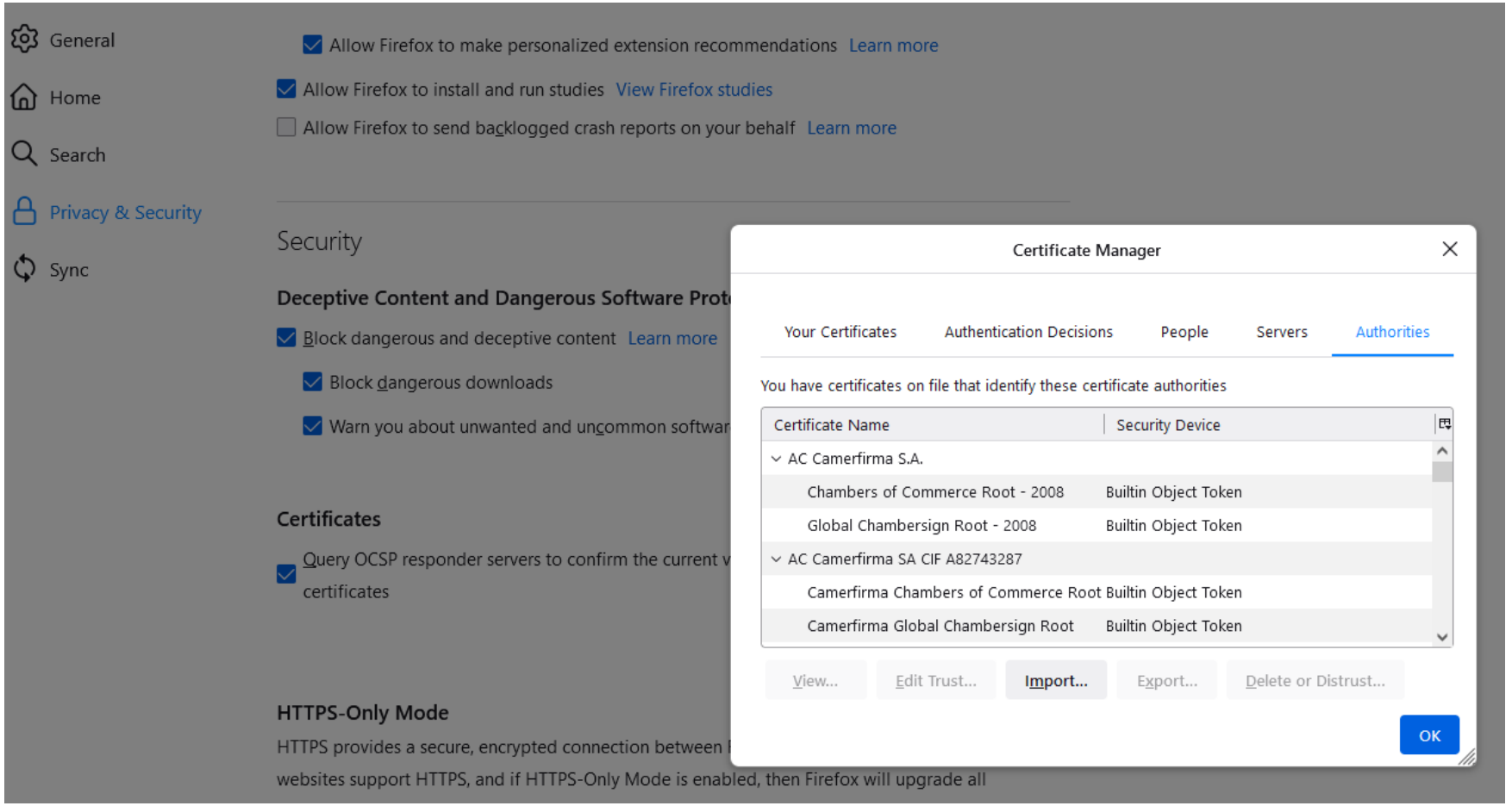
Browser Lists - Chrome

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

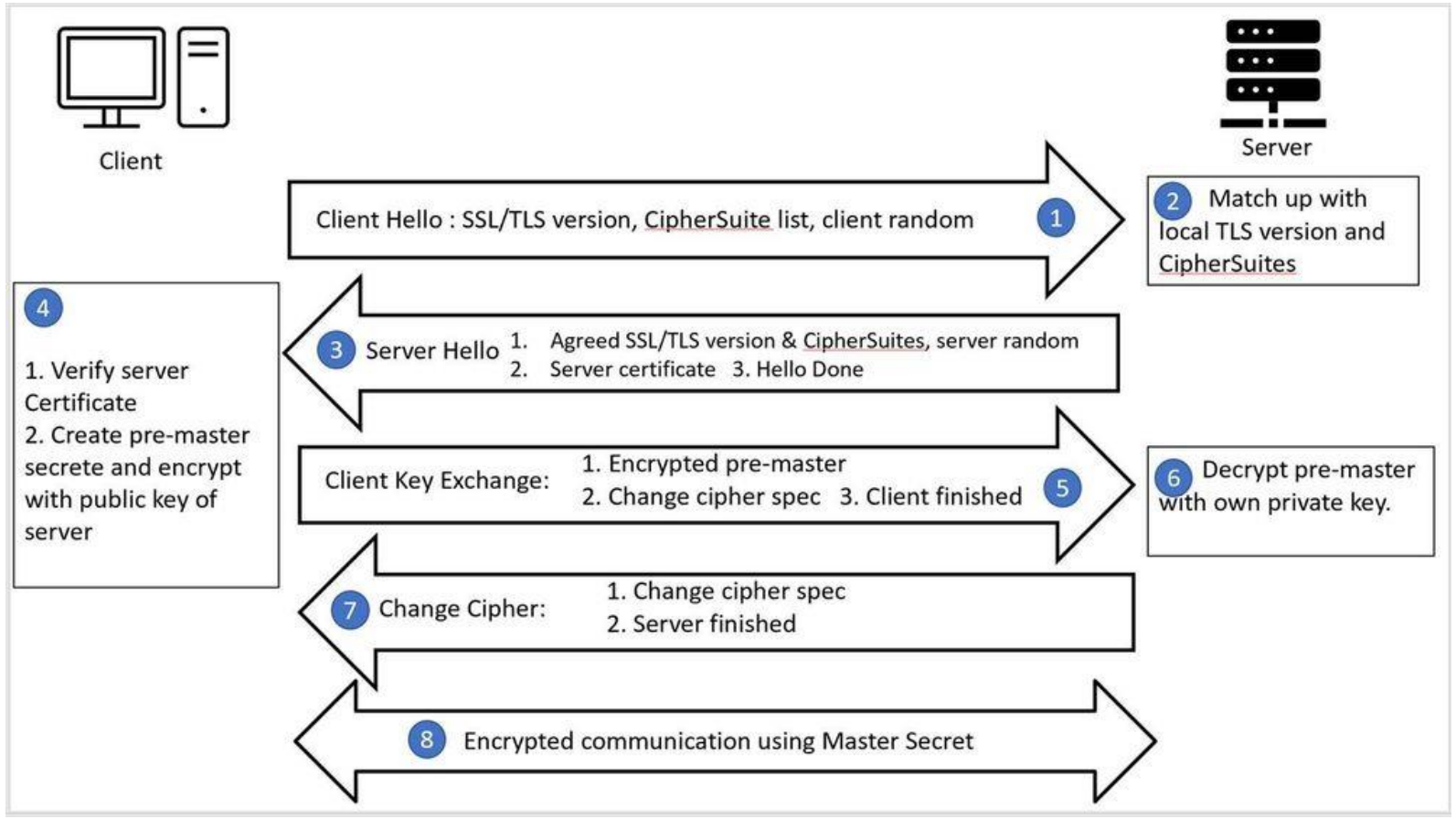


Browser Lists - Firefox

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering



TLS



Source: Microsoft