

CECS 303:

Networks and Network

Security

PKI

Chris Samayoa

Week 15 – 1st Lecture
4/26/2022

Course Information

- 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

- 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)



BOB



Public Key



Private Key

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

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



ALICE

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

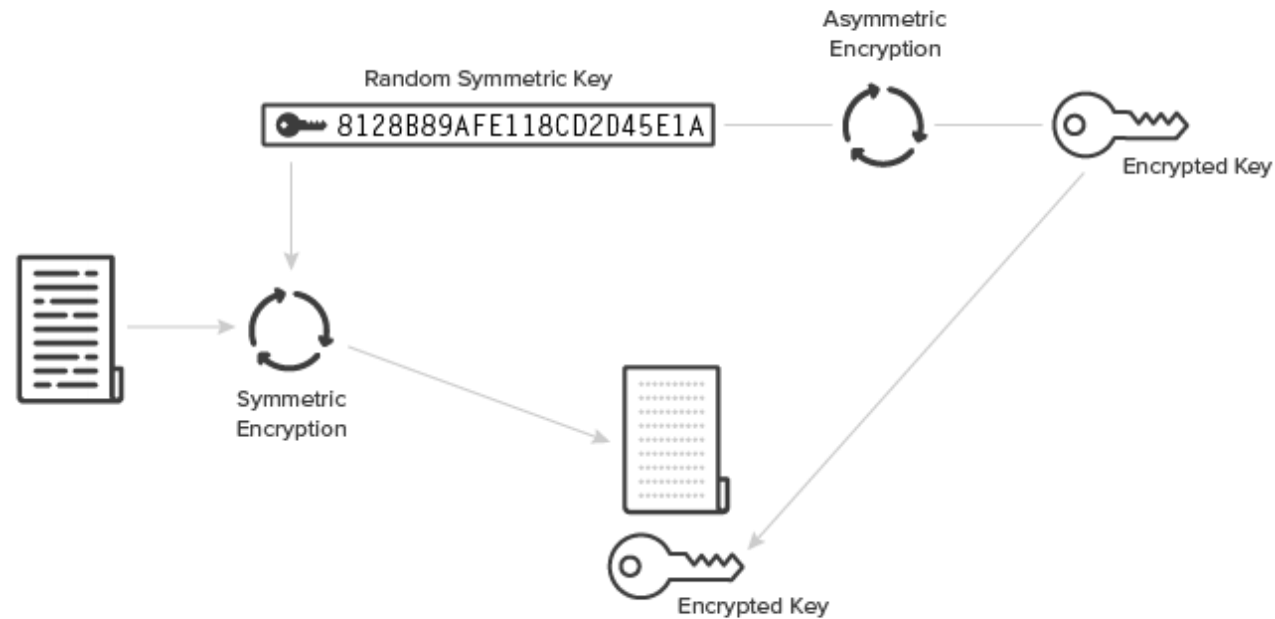
Bitcoin / Blockchain

Signal Private Messenger

Public Key Infrastructure

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

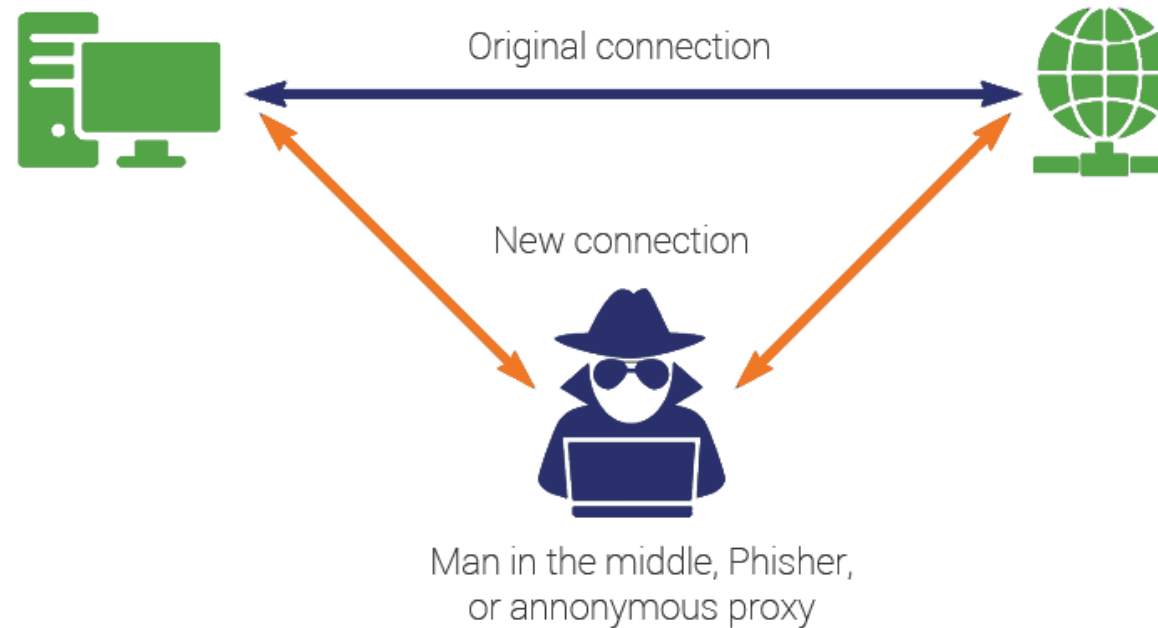


Objectives

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

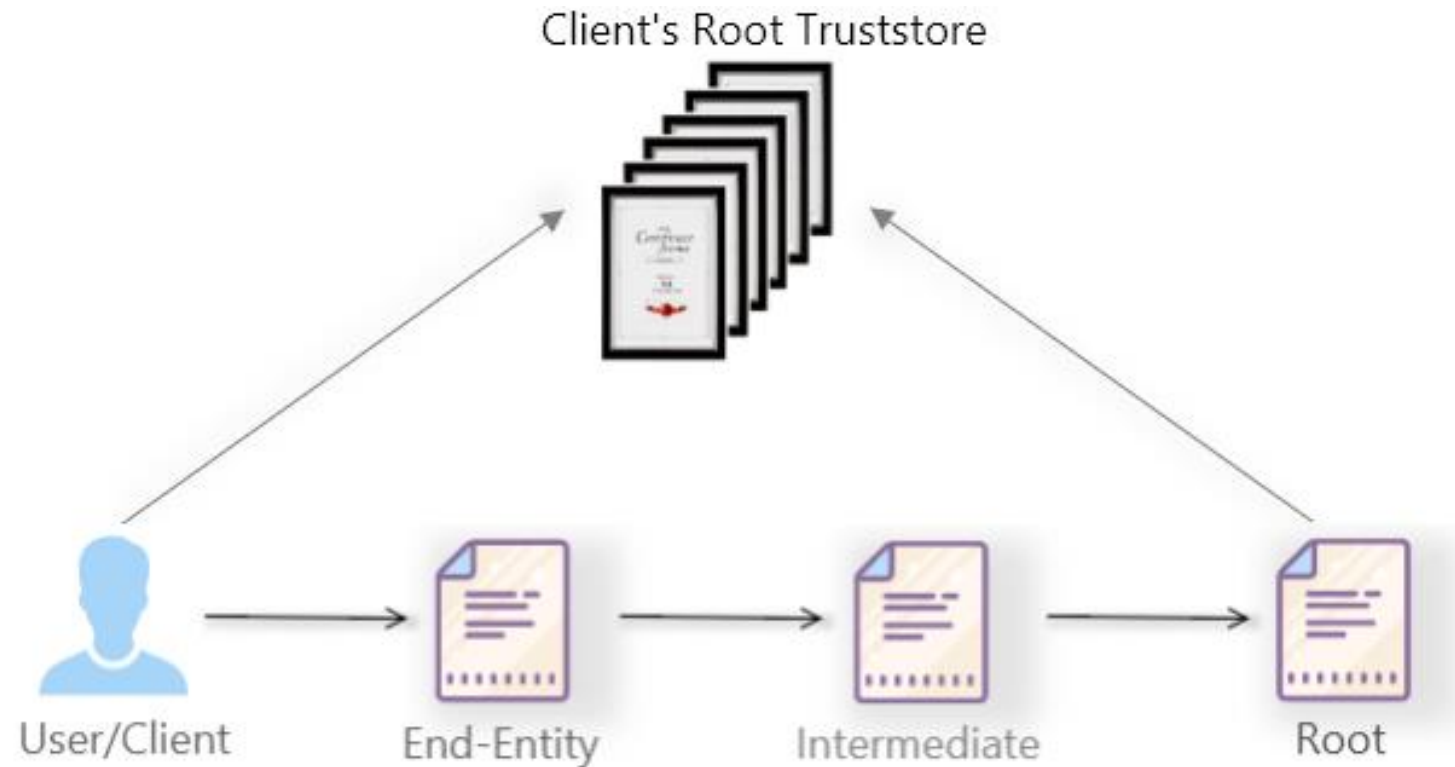
PKI Problem

- 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



PKI Solution

- Trusted third party



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

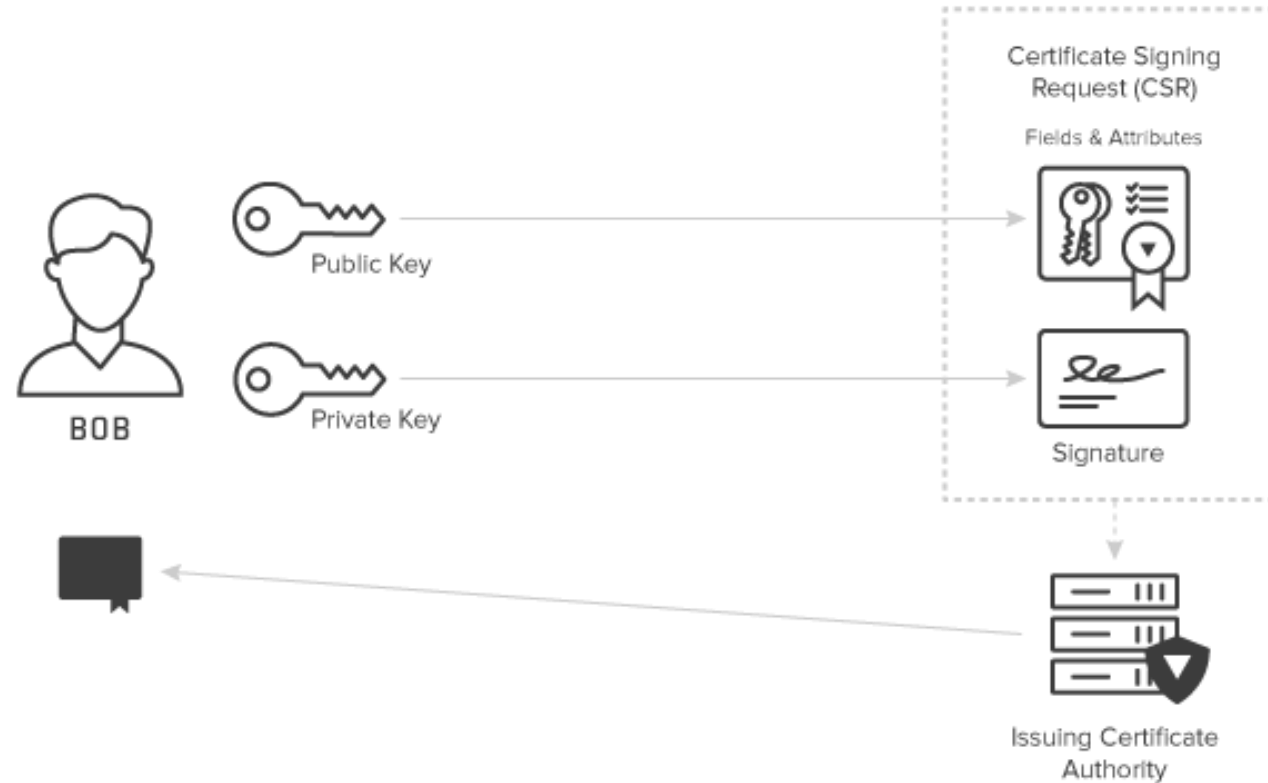
Certificate Authority

- 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

Certificate Authority (cont'd)



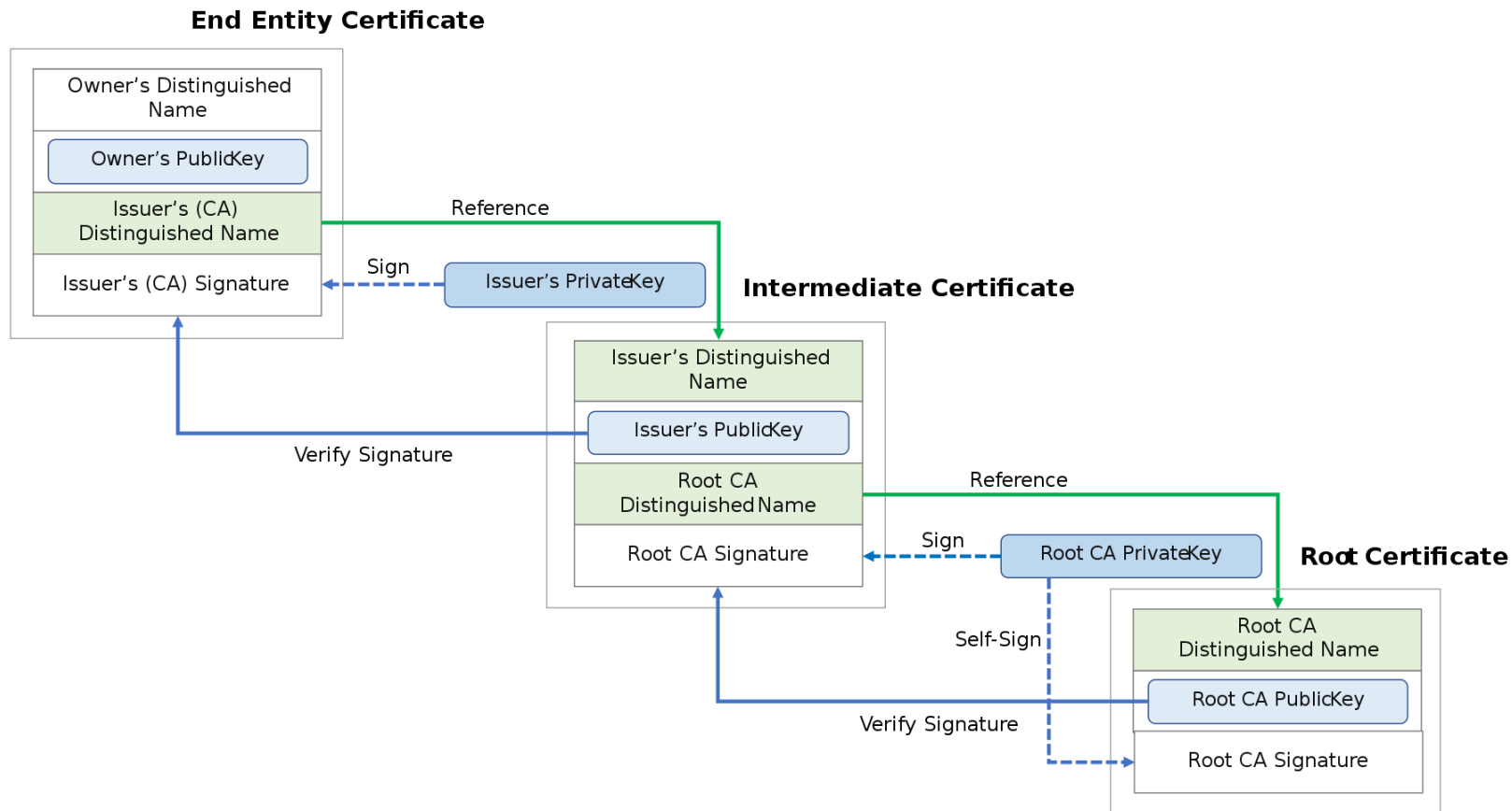
CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering



Objectives

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

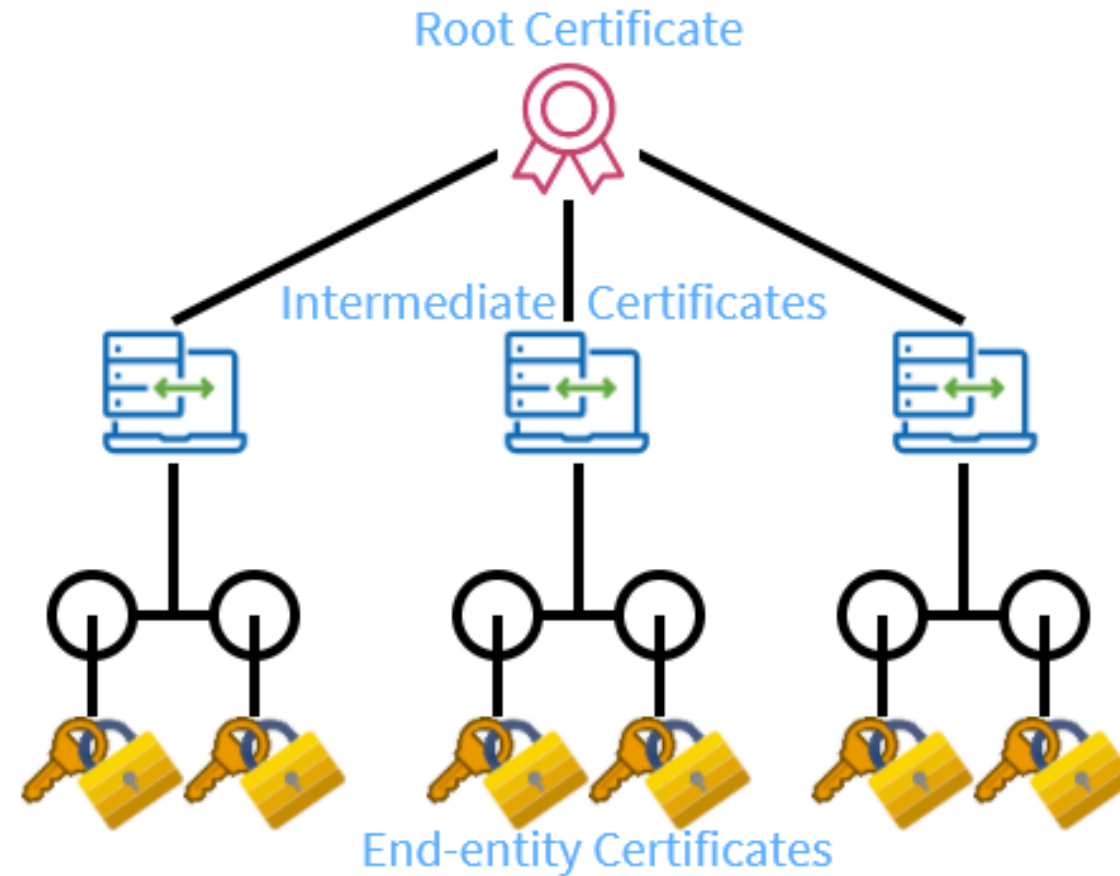
PKI Chain of Trust



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)

Typical Trust Model



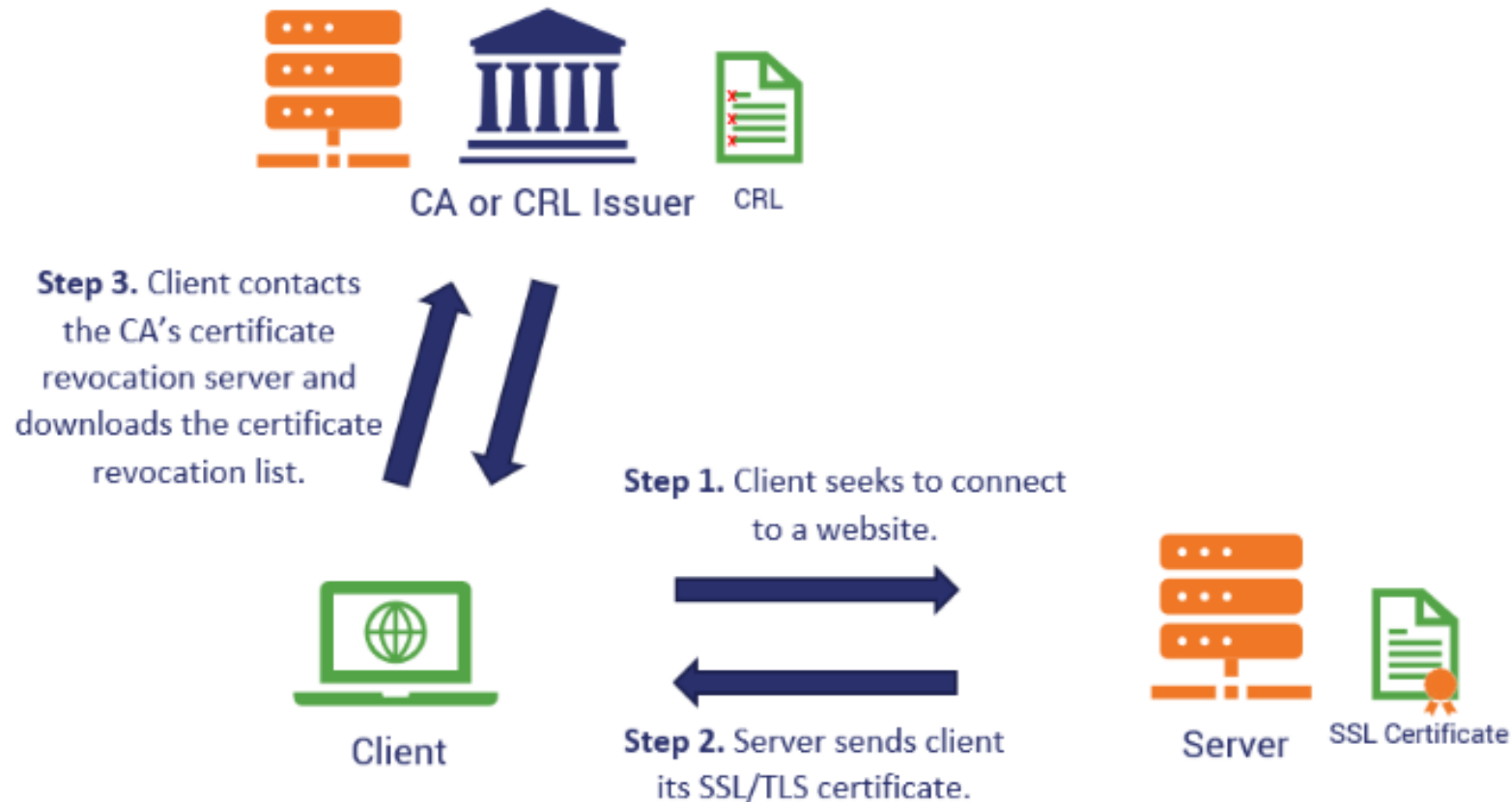
Digital Certificate Risks

- 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



Browser Lists - Chrome



Settings

manage certificates

Help improve security on the web for everyone
Sends URLs of some pages you visit, limited system information, and some page content to Google, to help discover new threats and protect everyone on the web.

cards are exposed in a data breach
checks your passwords against lists that have been published online.
ur passwords and usernames are encrypted, so they can't be read by
oogle.

recommended)
u against dangerous websites, downloads, and extensions. You'll still get Safe
y, where available, in other Google services, like Gmail and Search.

ctions
TPS and warn you before loading sites that don't support it

ct to websites over a secure connection

urrent service provider
may not be available all the time

With Custom
Enter custom provider

Manage phones
Control which phones you use as security keys

Manage certificates
Manage HTTPS/SSL certificates and settings

Certificates

Intended purpose: <All>

Intermediate Certification Authorities Trusted Root Certification Authorities Trusted Publi

Issued To	Issued By	Expiratio...	Friendly Name
AAA Certificate Ser...	AAA Certificate Services	12/31/2028	Sectigo (AAA)
Actalis Authenticati...	Actalis Authentication...	9/22/2030	Actalis Authentic...
AddTrust External ...	AddTrust External CA...	5/30/2020	Sectigo (AddTrust)
AffirmTrust Comme...	AffirmTrust Commercial	12/31/2030	AffirmTrust Com...
Baltimore CyberTru...	Baltimore CyberTrust ...	5/12/2025	DigiCert Baltimor...
Bitdefender Person...	Bitdefender Personal ...	12/19/2031	<None>
Certum CA	Certum CA	6/11/2027	Certum
Certum Trusted Ne...	Certum Trusted Netw...	12/31/2029	Certum Trusted ...
Class 3 Public Prima...	Class 3 Public Primary ...	8/1/2028	VeriSign Class 3 ...

Import... Export... Remove Advanced

Certificate intended purposes
Client Authentication, Code Signing, Encrypting File System, Secure Email, IP security tunnel termination, IP security user, Server Authentication, Time Stamping View

Close

Browser Lists - Firefox



The screenshot shows the Firefox settings interface. On the left, a sidebar contains links for General, Home, Search, Privacy & Security, and Sync. The main content area is divided into sections: General (with checkboxes for extension recommendations, studies, and crash reports), Security (with checkboxes for blocking dangerous content and downloads, and warning about unwanted software), Certificates (with a checkbox for querying OSCP responder servers), and HTTPS-Only Mode. A 'Certificate Manager' dialog box is open in the foreground, displaying a table of certificate authorities. The dialog has tabs for 'Your Certificates', 'Authentication Decisions', 'People', 'Servers', and 'Authorities'. The 'Authorities' tab is selected, showing a list of certificate names and their security devices. The list includes 'AC Camerfirma S.A.' with two entries (Chambers of Commerce Root - 2008 and Global Chambersign Root - 2008) and 'AC Camerfirma SA CIF A82743287' with two entries (Camerfirma Chambers of Commerce Root and Camerfirma Global Chambersign Root). All entries are associated with 'Builtin Object Token'. At the bottom of the dialog are buttons for 'View...', 'Edit Trust...', 'Import...', 'Export...', 'Delete or Distrust...', and an 'OK' button.

General

- ☒ Allow Firefox to make personalized extension recommendations [Learn more](#)
- ☒ Allow Firefox to install and run studies [View Firefox studies](#)
- ☐ Allow Firefox to send backlogged crash reports on your behalf [Learn more](#)

Security

Deceptive Content and Dangerous Software Protection

- ☒ Block dangerous and deceptive content [Learn more](#)
- ☒ Block dangerous downloads
- ☒ Warn you about unwanted and uncommon software

Certificates

- ☒ Query OSCP responder servers to confirm the current validity of certificates

HTTPS-Only Mode

HTTPS provides a secure, encrypted connection between your browser and websites that support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all

Certificate Manager

Authorities

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

[View...](#) [Edit Trust...](#) [Import...](#) [Export...](#) [Delete or Distrust...](#) [OK](#)

TLS

