CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

PKI and DNSSEC

Chris Samayoa

Week 15 – 2nd Lecture
4/28/2022

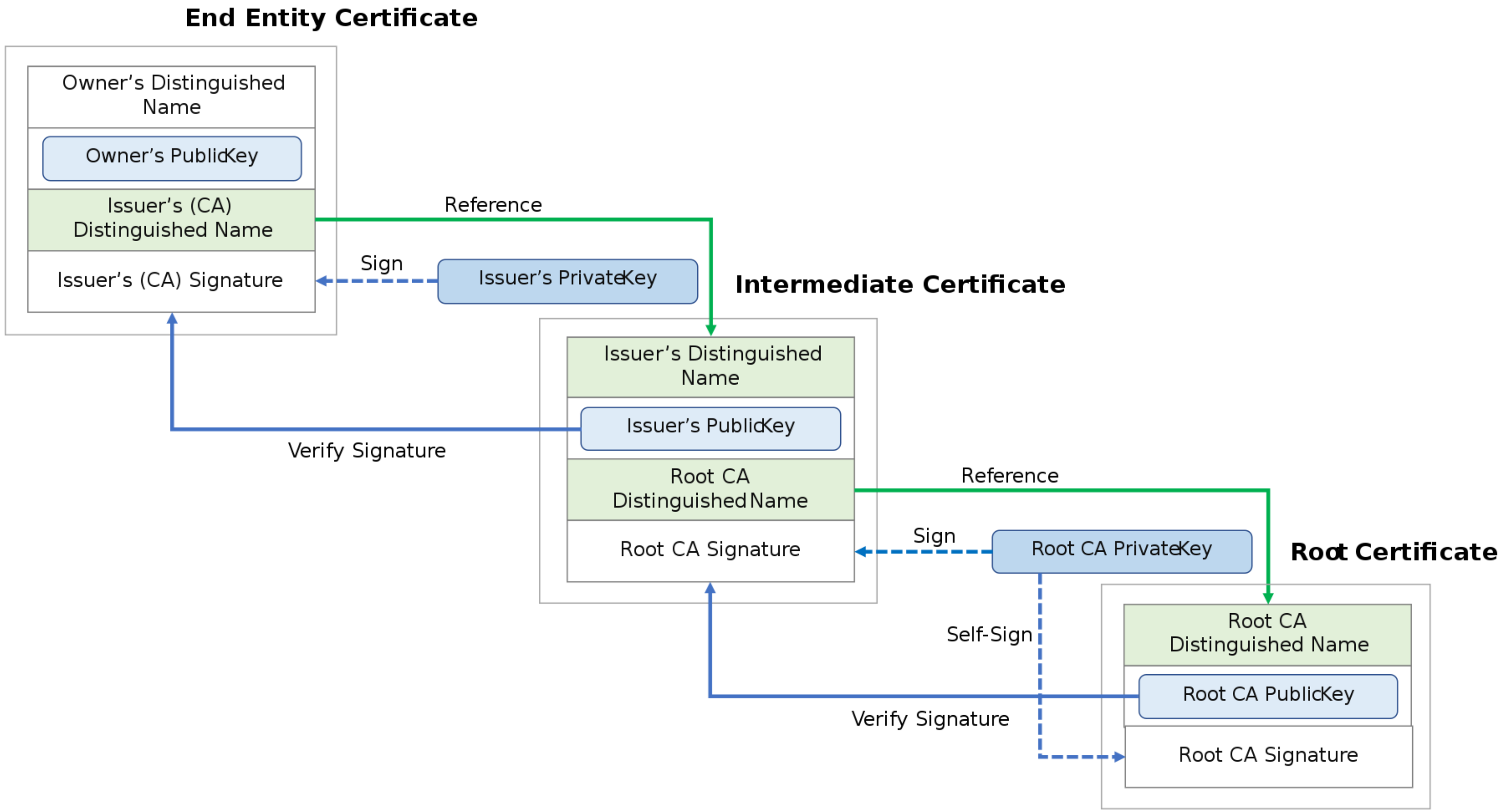
Course Information

- 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
  - Chain of Trust
- DNSSEC
  - Record Types
  - ZSK (Zone-signing Key)
  - KSK (Key-signing Key)
  - Chain of Trust

PKI Chain of Trust



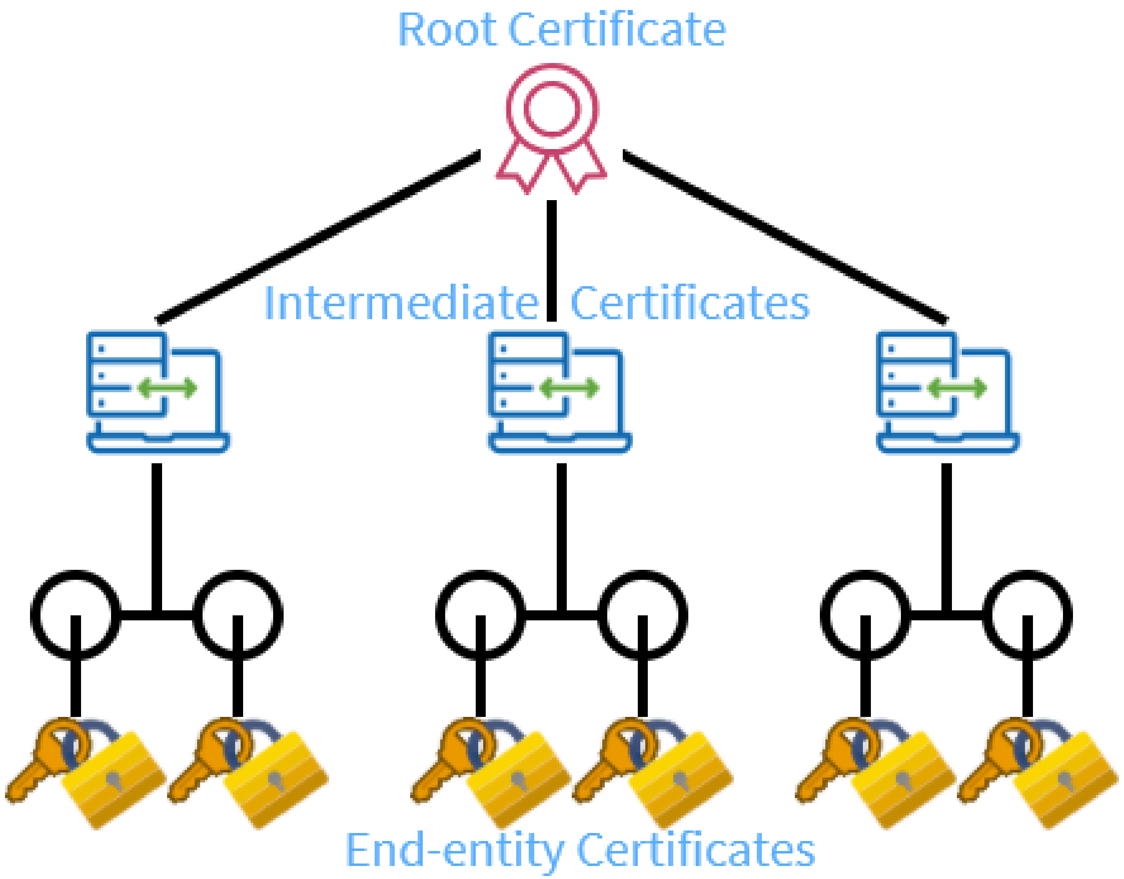
Source: https://en.wikipedia.org/wiki/Chain_of_trust#/media/File:Chain_Of_Trust.svg

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 directly to employees)
    - Parameters specified within certificate(s)

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

Typical Trust Model



Root Certificate

Intermediate Certificates

End-entity Certificates

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

CALIFORNIA STATE UNIVERSITY LONG BEACH
College of Engineering

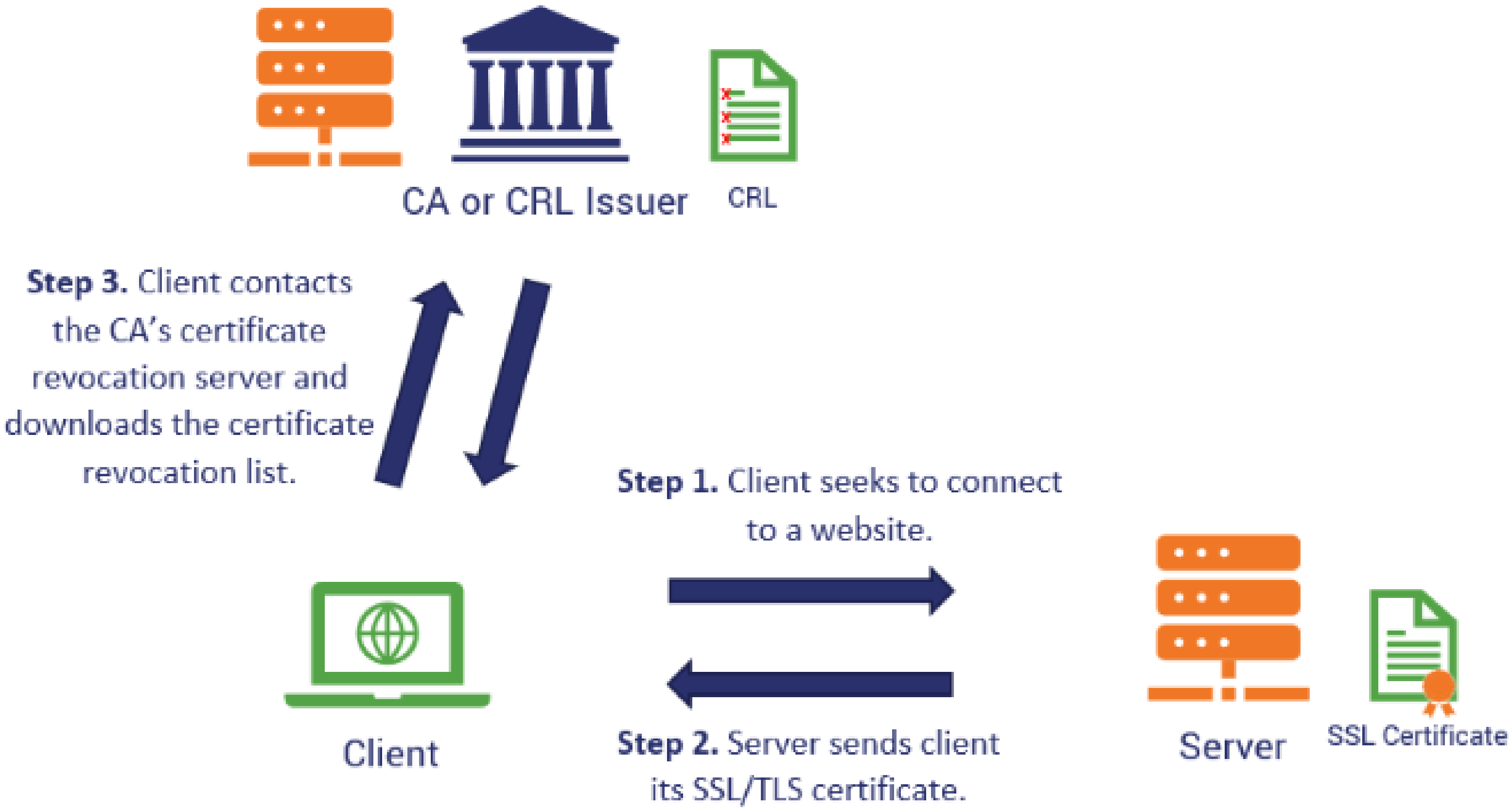
Digital Certificate Risks

- 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



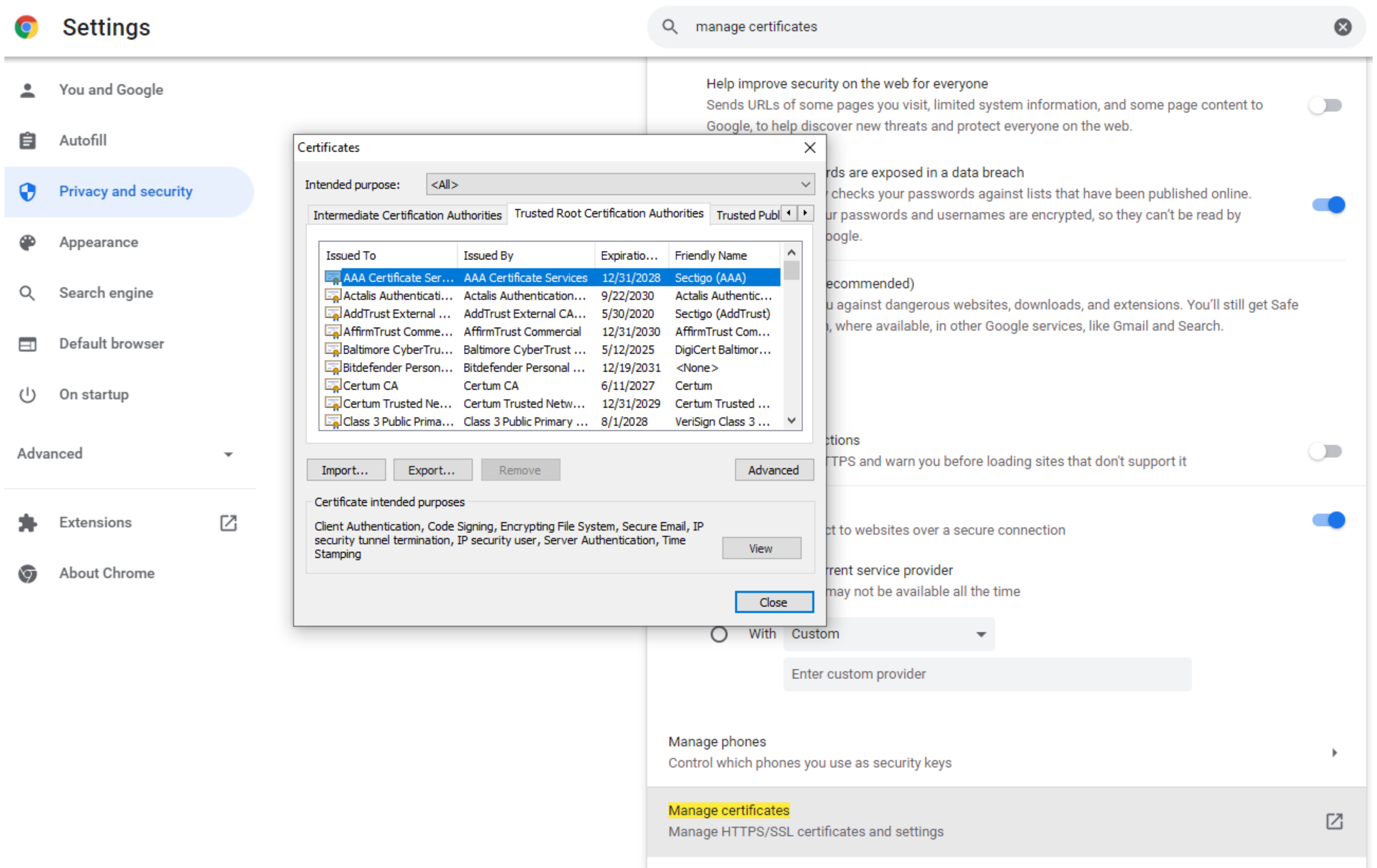
Step 3. Client contacts the CA's certificate revocation server and downloads the certificate revocation list.

Step 1. Client seeks to connect to a website.

Step 2. Server sends client its SSL/TLS certificate.

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

Browser Lists - Chrome



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.

rds 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.

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

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

t to websites over a secure connection

rent 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>

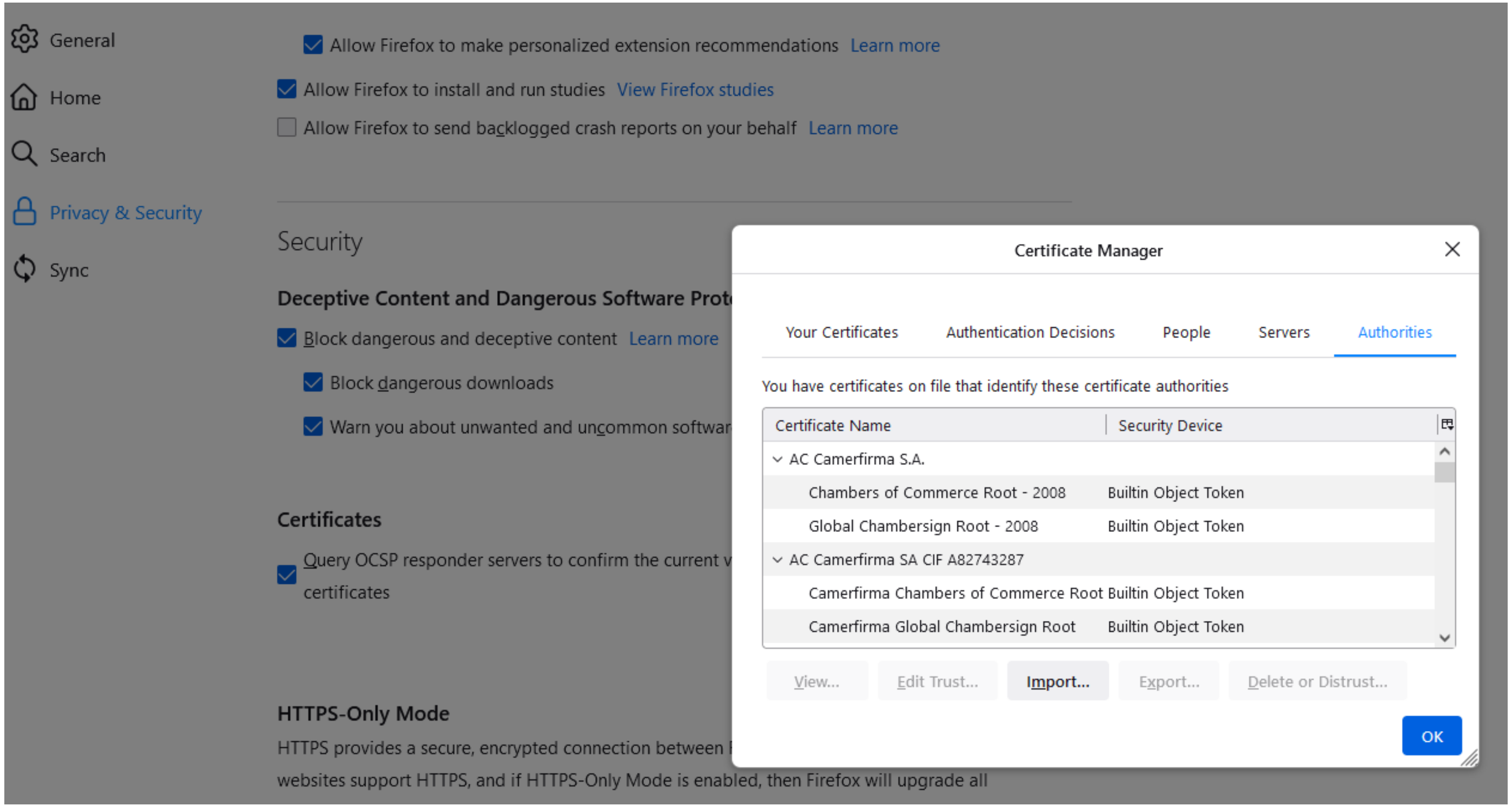
Intermediate Certification Authorities | Trusted Root Certification Authorities | Trusted Publ

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 ...

Certificate intended purposes

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

Browser Lists - Firefox



☑ 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 Prote

☑ Block dangerous and deceptive content Learn more

☑ Block dangerous downloads

☑ Warn you about unwanted and uncommon softwar

Certificates

☑ Query OCSP responder servers to confirm the current v certificates

HTTPS-Only Mode

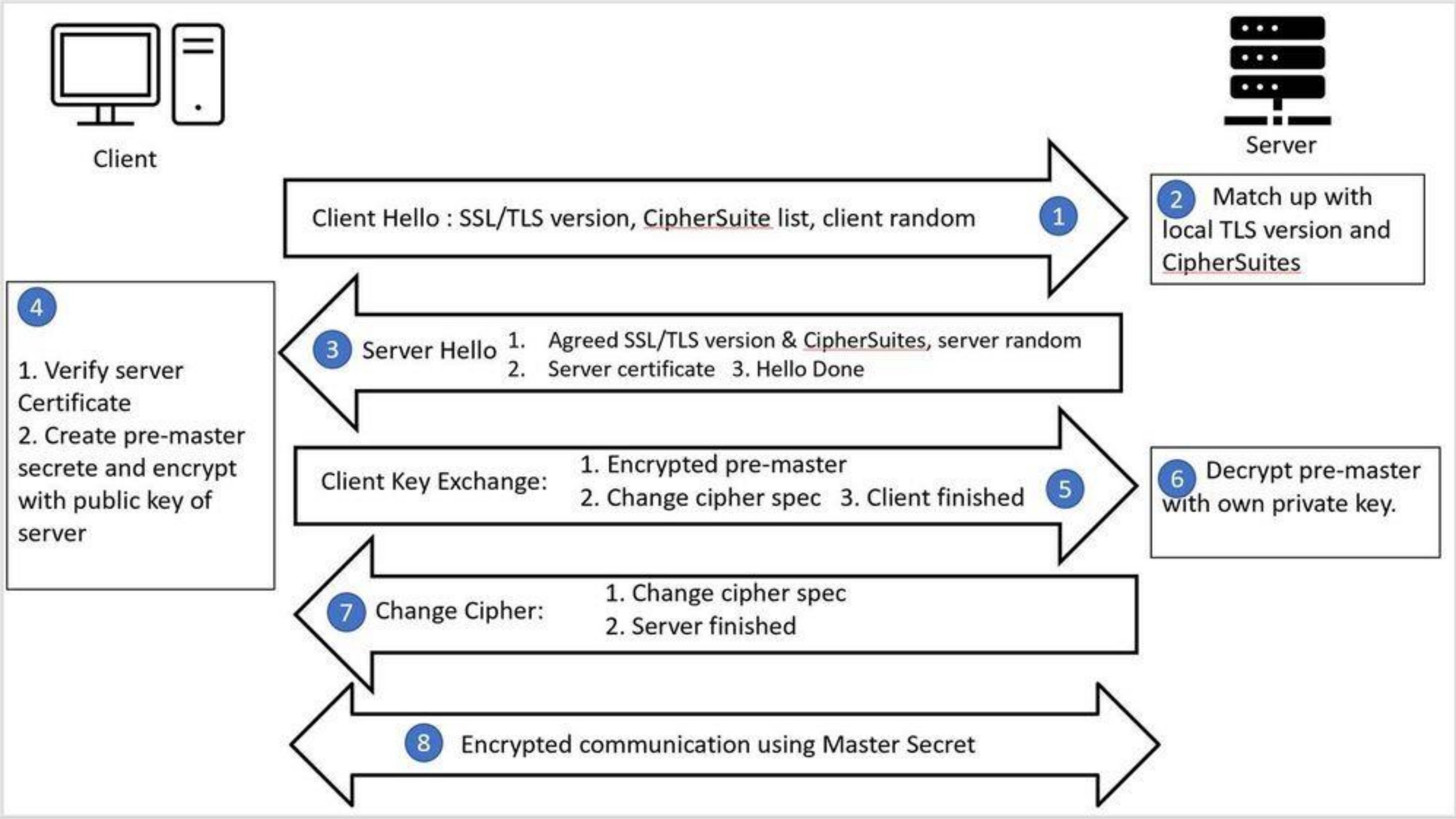
HTTPS provides a secure, encrypted connection between websites support HTTPS, and if HTTPS-Only Mode is enabled, then Firefox will upgrade all

Certificate Manager

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

TLS



Client

Server

1 Client Hello : SSL/TLS version, CipherSuite list, client random

2 Match up with local TLS version and CipherSuites

3 Server Hello 1. Agreed SSL/TLS version & CipherSuites, server random 2. Server certificate 3. Hello Done

4 1. Verify server Certificate 2. Create pre-master secrete and encrypt with public key of server

5 Client Key Exchange: 1. Encrypted pre-master 2. Change cipher spec 3. Client finished

6 Decrypt pre-master with own private key.

7 Change Cipher: 1. Change cipher spec 2. Server finished

8 Encrypted communication using Master Secret

Source: Microsoft

Objectives

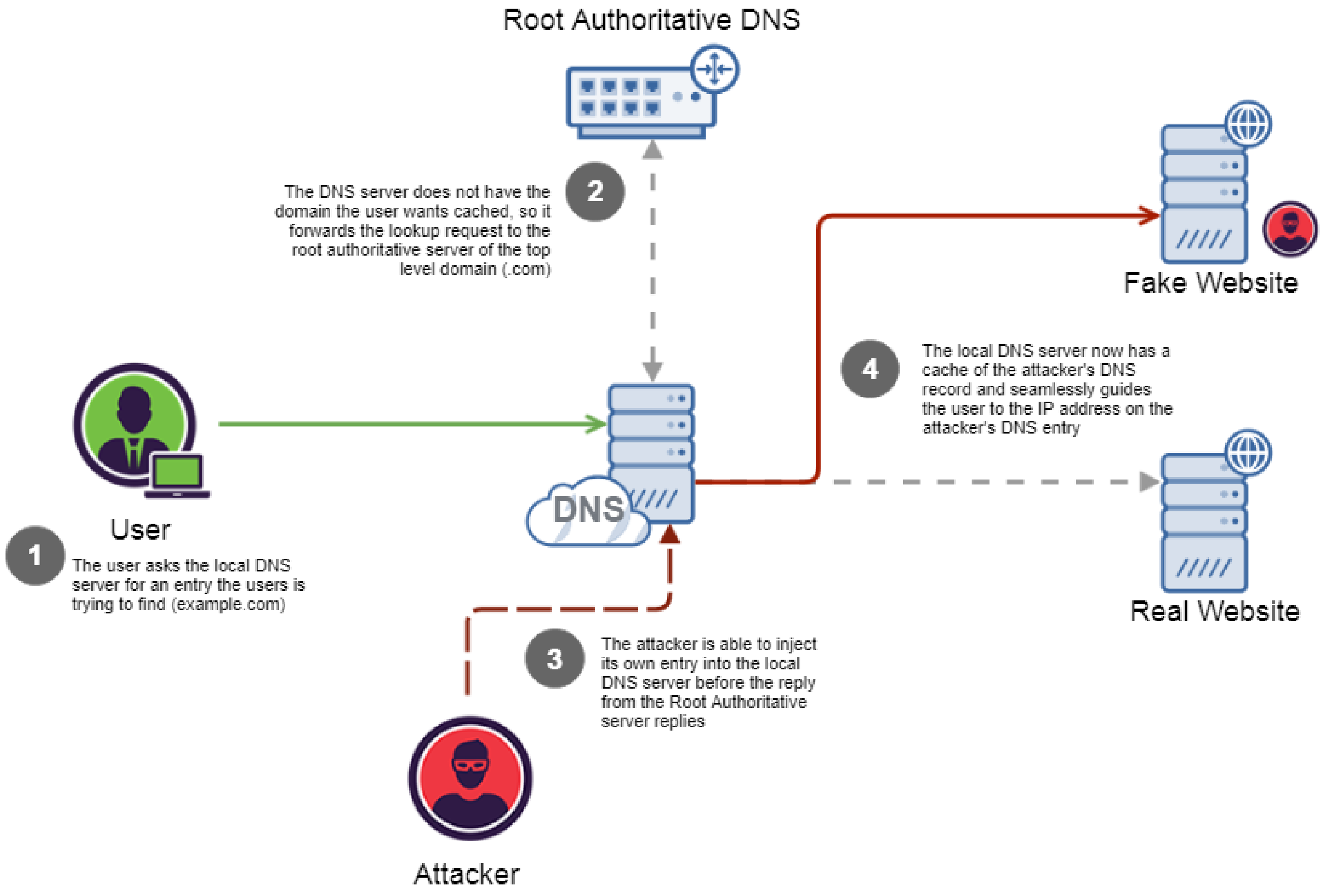
- PKI
  - Chain of Trust
- DNSSEC
  - Record Types
  - ZSK (Zone-signing Key)
  - KSK (Key-signing Key)
  - Chain of Trust

DNSSEC

- Background
  - Security not a primary design consideration for DNS initially
    - No authentication for DNS query responses
    - Source IP of expected DNS server can be spoofed
  - IETF RFC 3757, 4033, 4034, 4035, 4509, 4641, 5155
  - DNS Cache Poisoning
    - If recursive resolver accepts false DNS response, then any devices querying for the data will be sent the incorrect address
- DNS Security Extensions (DNSSEC)
  - Suite of extensions meant to strengthen DNS security
  - Strengthens DNS authentication using digital signatures
    - Based on PKI
  - DNS data itself is signed by owner of data
  - Each DNS zone has public/private key pair
    - Each zone owner signs DNS data within the zone using the private key
    - Public key can be used by any resolver to validate the authenticity of DNS data received
  - Failure to authenticate signature results in discarded data and an error
- Two most important features added
  - Data origin authentication – verify that the data received came from the expected zone
  - Data integrity protection – resolver can ensure that they data received has not been modified in transit

Source: ICANN

DNS Cache Poisoning



2 The DNS server does not have the domain the user wants cached, so it forwards the lookup request to the root authoritative server of the top level domain (.com)

1 The user asks the local DNS server for an entry the users is trying to find (example.com)

3 The attacker is able to inject its own entry into the local DNS server before the reply from the Root Authoritative server replies

4 The local DNS server now has a cache of the attacker's DNS record and seamlessly guides the user to the IP address on the attacker's DNS entry

Source: https://medium.com/iocscan/dns-cache-poisoning-bea939b5afaf

Objectives

- PKI
  - Chain of Trust
- DNSSEC
  - Record Types
  - ZSK (Zone-signing Key)
  - KSK (Key-signing Key)
  - Chain of Trust

DNSSEC (cont'd)

- DNSSEC resource record types
  - RRSIG (Resource Record Signature)
    - Contains cryptographic signature for a given record set
  - DNSKEY
    - Holds the zone's public key
    - Used to verify signatures of zone's other records
    - Authoritative name server previously used private key to sign records
  - DS (Delegation Signer)
    - Used to verify delegation of DNS authority for child zones
  - NSEC (Next Secure record)
    - Returns next valid record name to prove that a particular DNS record does not exist
  - NSEC 3 (Next Secure version 3 record)
    - Hashes all record names in a zone (resolved NSEC-walking problem)
  - NSEC3PARAM (NSEC3 Parameter)
    - Specifies which NSEC3 records to include in responses for non-existent names
  - More information: https://simpledns.plus/help/dns-record-types

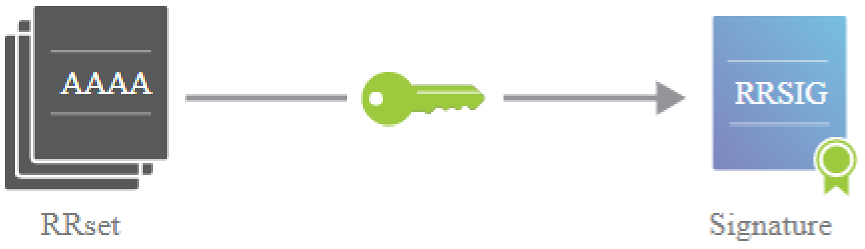
Source: https://www.imperva.com/learn/application-security/dnssec/

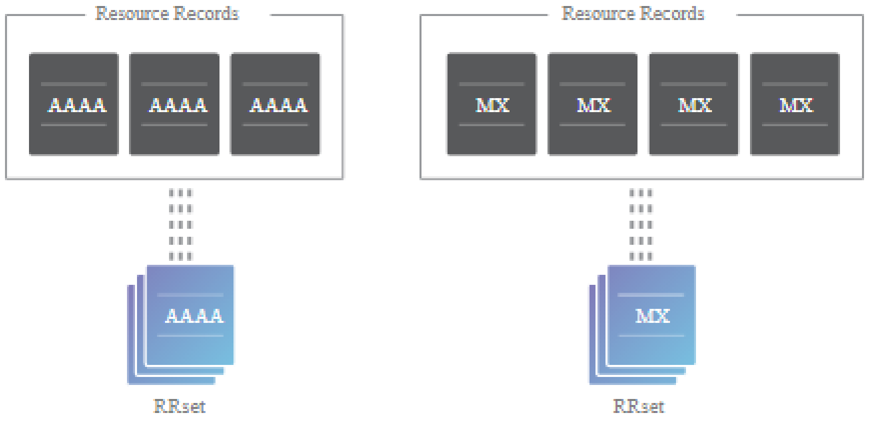
Objectives

- PKI
  - Chain of Trust
- DNSSEC
  - Record Types
  - ZSK (Zone-signing Key)
  - KSK (Key-signing Key)
  - Chain of Trust

Zone-Signing Keys

- Each zone has a Zone-Signing Key (ZSK) pair
  - Used to sign data in a zone routinely
  - Can be updated with no interaction outside of the zone it serves
  - Private portion signs each RRset
    - Public portion used to verify signature
    - Public key stored in zone operator's DNSKEY record
  - Signed RRset stored as RRSIG records
  - RRset
    - Grouping of same type of resource records within a zone

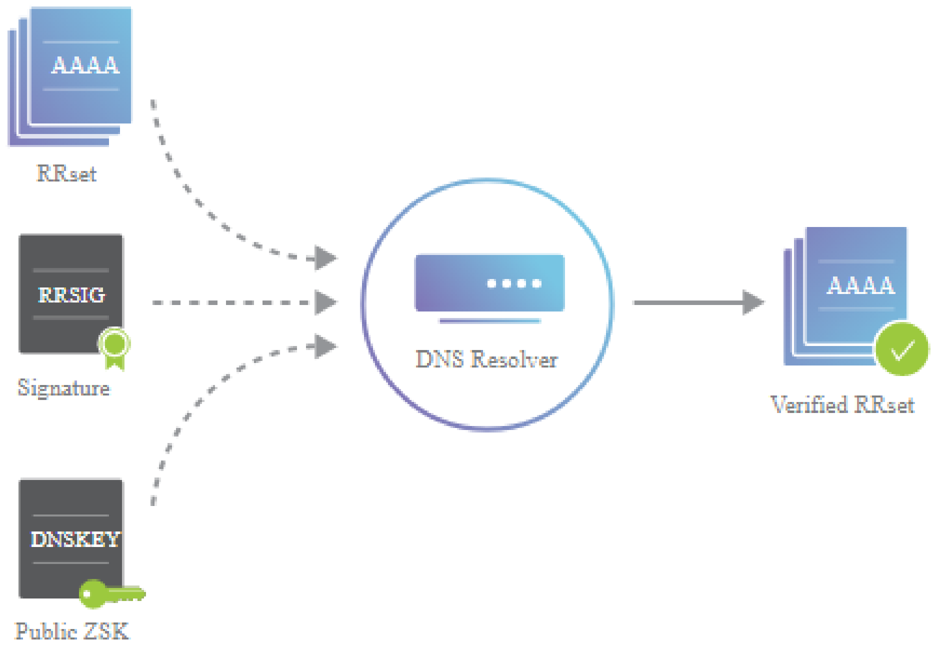




Source: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/

ZSK (cont’d)

- How is public ZSK used by a DNSSEC resolver?
  - When a record type is requested (e.g. A record), the answer returns along with the appropriate RRSIG
    - ➢ Resolver can then request the zone’s DNSKEY record (public ZSK) to validate the response received



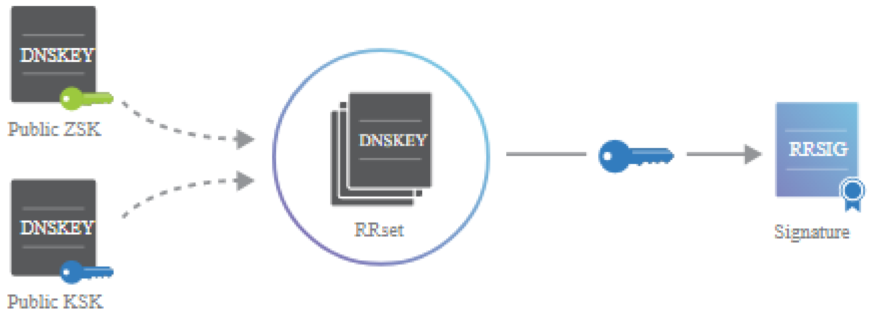
Source: https://www.imperva.com/learn/application-security/dnssec/

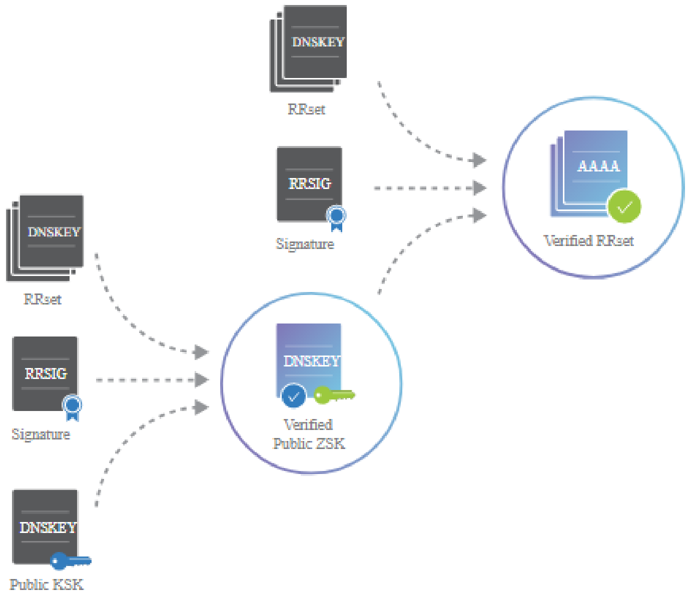
Objectives

- PKI
  - Chain of Trust
- DNSSEC
  - Record Types
  - ZSK (Zone-signing Key)
  - KSK (Key-signing Key)
  - Chain of Trust

Key-Signing Keys

- Key-signing Key (KSK) is used to validate the DNSKEY record for the requested zone
  - Only used to sign DNSKEY RRsets
  - This key needs action outside of zone to be updated
  - Used to sign the public ZSK
    - Separate DNSKEY record
    - RRset exists for public ZSK and public KSK
- Validate process for DNSSEC record is as follows:
  - RRset requested
    - Returned with corresponding RRSIG record
  - Request DNSKEY with public ZSK and public KSK
    - Returned with RRSIG for DNSKEY Rrset
  - RRSIG of requested RRset verified with public ZSK
  - RRSIG of DNSKEY RRset verified with public KSK





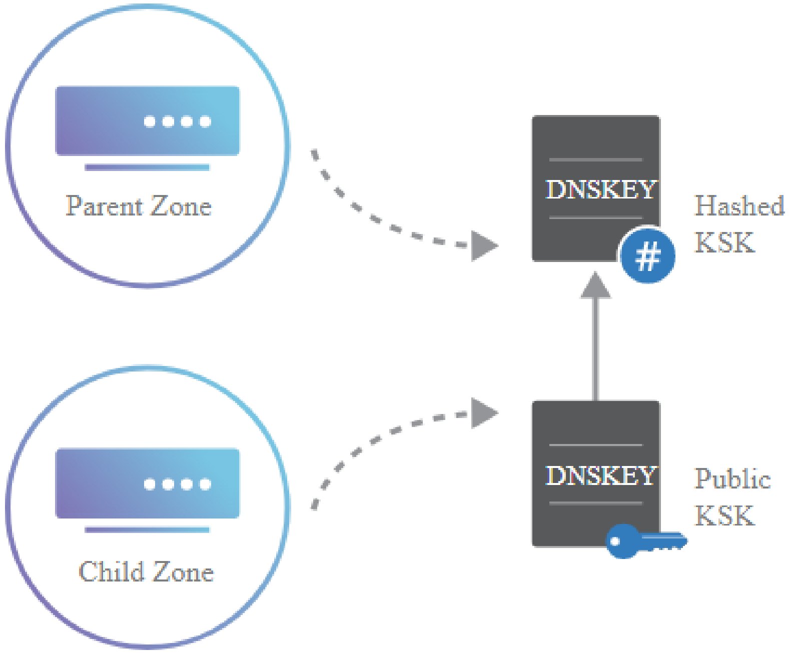
Source: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/

Objectives

- PKI
  - Chain of Trust
- DNSSEC
  - Record Types
  - ZSK (Zone-signing Key)
  - KSK (Key-signing Key)
  - Chain of Trust

Delegation Signer (DS) Record

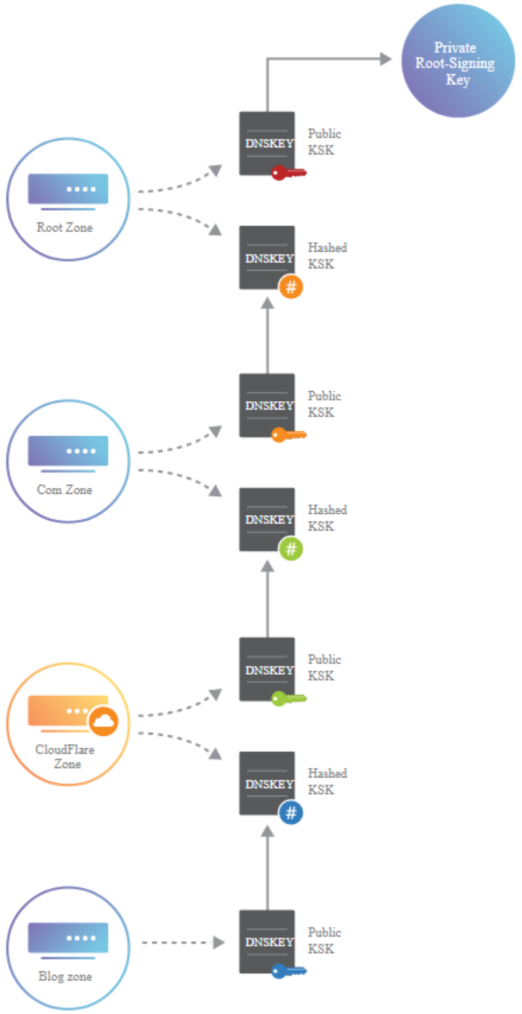
- DS record transfers trust from a parent zone to a child zone
  - e.g. ".com" can transfer trust for "cecs303.com" from it's own authoritative DNS servers to one chosen by the zone operator for "cecs303.com"
- KSK use between zones
  - Zone operator hashes DNSKEY record and provides it to the parent zone to be stored as a DS record
    - When parent zone redirects a request to a child zone, it also provides the corresponding DS record
  - Resolver can verify validity of child zone's public KSK by hashing it and comparing it to the parent zone's corresponding DS record
  - Change of KSK in any given zone requires that the parent zone's DS record be updated



Source: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/

DNSSEC Chain of Trust

- Similar to Chain of Trust used for SSL/TLS Certificate Authorities
  - Uses PKI
  - “Trust Anchor” necessary to establish chain of trust
    - ICANN maintains a trusted root server for DNSSEC
      - Public KSK often used as trusted root server (trust anchor)
    - DNSSEC enabled resolver must have at least one trust anchor’s public key installed
      - Similar to trusted root CAs in web browsers
    - Root signed in public and highly auditable manner to produce RRSIG at that level
- DS records are also signed and have a corresponding RRSIG record
  - This allows for a repeatable process to validate signatures until the root is reached



Source: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/

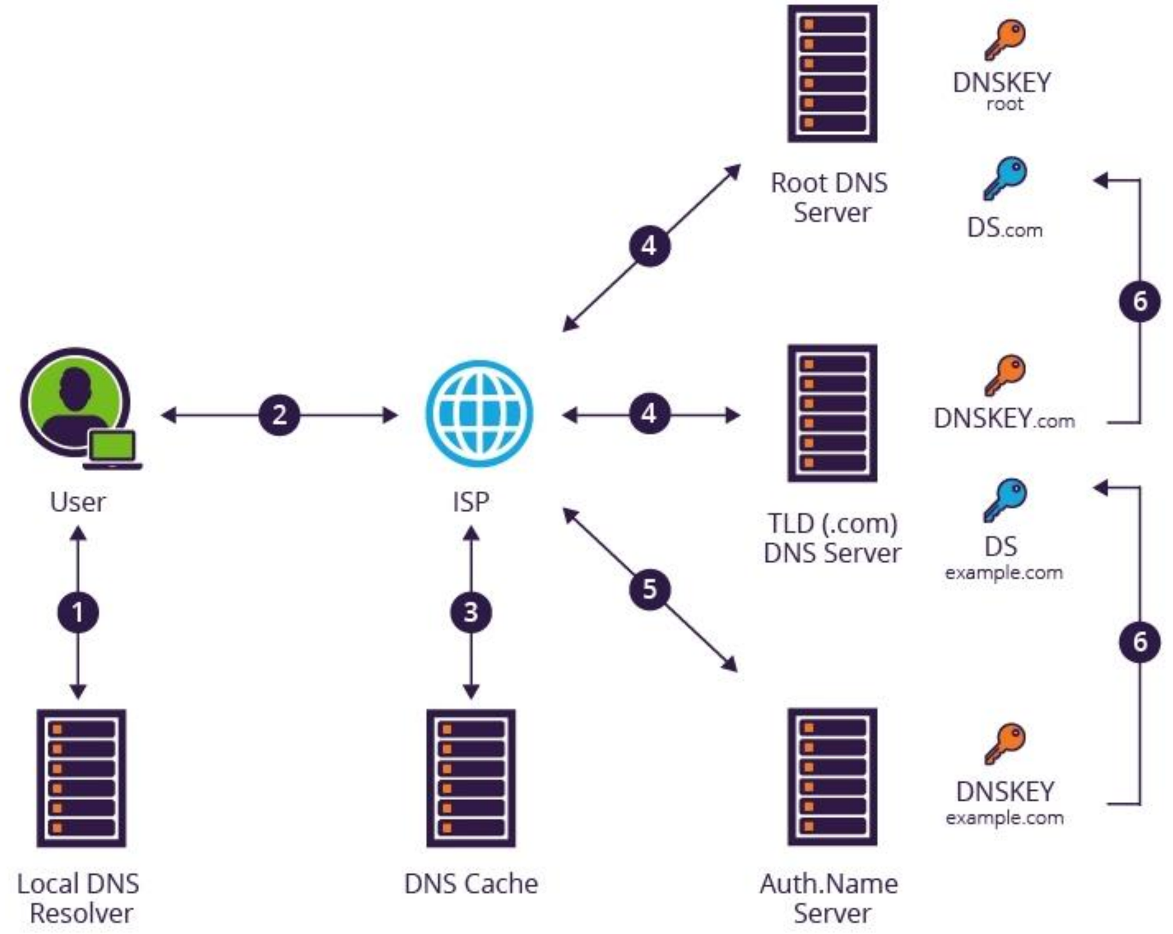
DNSSEC Process Summary

- User requests a URL (e.g. abc.com)
  - Kicks off query to local DNS server
    - IP address returned to browser if cached
  - If not cached locally, then request made to a recursive resolver (e.g. ISP’s DNS server)
    - IP address returned to browser if cached at this level
    - Otherwise, recursive query launched to find authoritative DNS server for requested domain
- Recursive resolver contacts root DNS server to find top-level domain (TLD) DNS server for requested domain
  - e.g. “abc.com”s TLD would be “.com”
- TLD DNS server redirects to the authoritative name server for the requested domain
  - Authoritative name server for requested domain holds a list of DNS records for it (e.g. www.abc.com A record)
- During each step of this search, a corresponding DNSSEC record is requested by the resolver
  - e.g. for “abc.com” query -> RRSET, RRSIG, and public ZSK are obtained
    - RRSIG is validated using public ZSK
    - ZSK DNSKEY record (public key) is requested and validated using public KSK key (also a DNSKEY record)
    - KSK public key validated by checking parent zone’s corresponding DS record for domain
- One DNSSEC validation has concluded, DNS request with the correct IP address is sent to client

Source: https://www.imperva.com/learn/application-security/dnssec/

DNSSEC Process Summary

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering



Source: https://www.imperva.com/learn/application-security/dnssec/