# Revocation: Expiration Dates

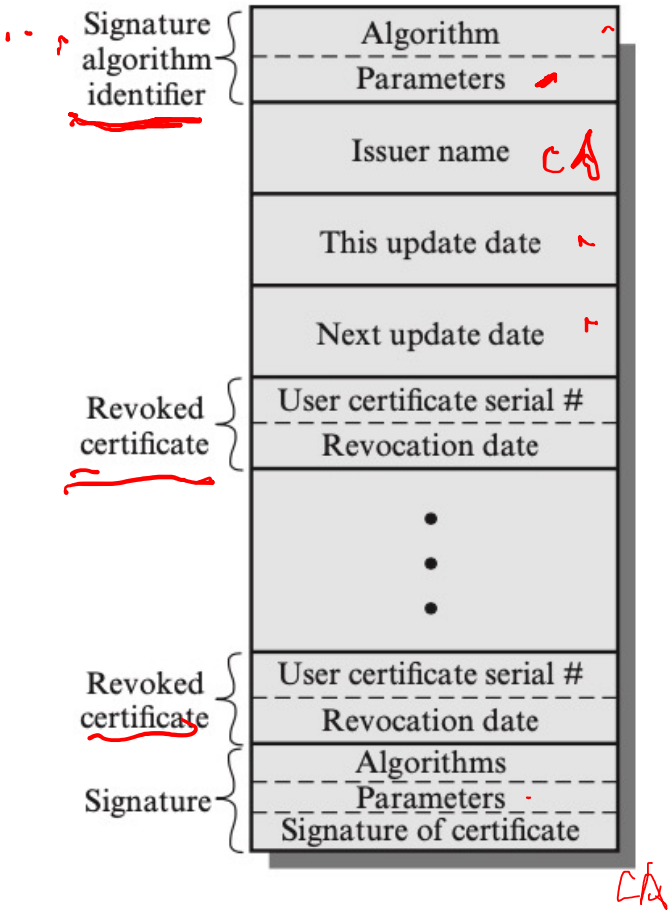
- Approach I: Each certificate has an expiration date
  - As a certificate nears expiration or is compromised, the owner must request a new one from the CA
  - Once expired, a compromised or invalid certificate automatically becomes unusable – even if it wasn't explicitly revoked.
- Benefits
  - Mitigates damage: Eventually, the bad certificate will become harmless
- Drawbacks
  - Adds management burden: Everybody has to renew their certificates frequently
  - If someone forgets to renew a certificate, their website might stop working
- Tradeoff: How often should certificates be renewed?
  - Frequent renewal: More secure, less usable – adds maintenance complexity
  - Infrequent renewal: Less secure, more usable – extends the risk window for compromised certificates
  - *Let's Encrypt* (a certificate authority) chose very frequent renewal before 2022
    - Let's Encrypt is a non-profit certificate authority run by Internet Security Research Group that provides X.509 certificates for Transport Layer Security encryption at no charge.

# Revocation: Announcing Revoked Certificates

- Approach II: Periodically release a list of invalidated certificates
  - Users must periodically download a Certification Revocation List (CRL)
- How do we authenticate the list?
  - The certificate authority signs the list!
    - {"The certificate with serial number 0xdeadbeef is now revoked"}$_{SK_{CA}^{-1}}$
- Drawbacks
  - Lists can get large - all revoked certificates that have not yet expired.
    - Mitigated by shorter expiration dates (don't have to list them once they expire)
  - Until a user downloads a list, they won't know which certificates are revoked
- What happens if the certificate authority is unavailable?
  - Fail-safe default: Assume all certificates are invalid? Now we can't trust anybody!
    - Possible attack: Attacker forces the CA to be unavailable (denial of service attack)
  - Use old list: Potentially dangerous if the old list is missing newly revoked certificates

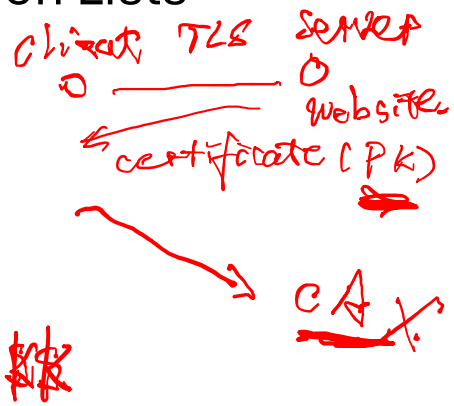
# X.509 certificate revocation list

- CA maintain a list of all revoked but not expired certificates and post them to directory
- Revoked list is designed by issuer
- When receiving a certificate, user searches revoked list in a local cache



# Revocation: Online Certificate Status Protocol (OCSP)

- 🔒 Approach III OCSP: Check **if a digital certificate is still valid or revoked —** without downloading large Certificate Revocation Lists (CRLs).
- ⚙️ **How It Works**
  1. **Browser/Client** connects to a secure website (HTTPS).
  2. It queries the **OCSP responder** (run by the Certificate Authority): "Is this certificate still valid?"
  3. The **OCSP responder** replies with one of:
     1. ✅ **Good** – Certificate is valid
     2. ❌ **Revoked** – Certificate has been invalidated
     3. ⚠️ **Unknown** – Not recognized by CA
- **Problems of traditional OCSP:**
  - ❌ Extra network latency (one more connection)
  - ❌ Privacy leak (CA sees which sites users visit)
  - ❌ Potential failures if OCSP server is unreachable

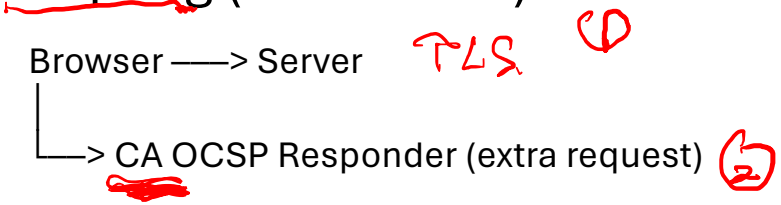


# Revocation: OCSP Stapling (Improved Method)

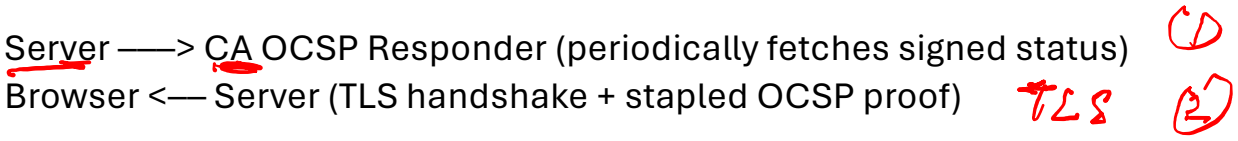
- Approach IV: OCSP stapling is a **server-side enhancement** to the OCSP, designed to make certificate status checking **faster, more private, and more reliable**.
- OCSP Stapling Flow
  - The **server** periodically contacts the CA's OCSP responder to obtain a **signed OCSP response**.
  - The server **caches** this response for a limited time (typically 1–7 days).
  - During the TLS handshake, the server **"staples"** this OCSP response to its certificate.
  - The **browser** verifies the signature on the stapled response — no need to contact the CA.

# OCSP Stapling Benefits

- Without Stapling (Traditional)




- With Stapling




- ✅ Faster page loads (no client-side OCSP lookup)
- ✅ Improved privacy (browser never contacts CA directly)
- ✅ Reduced CA server load and better reliability

# Summary

- Certificate – created by CA
  - X.509
- Obtaining a User Certificate
  - Trusted Directory – maintain & store certificates
  - Scalability issue – hierarchical trust/CAs by delegating trust and signing power to intermediate CAs
- Revocation
  - Use the expiration date
  - Revocation List
  - Online Certificate Status Protocol (OCSP)
  - OCSP stapling

# Homework 3 - individual

- Chapter 4
- **Deadline**: Friday,  Nov 21, 2025, at 11: 59 PM
- We will use the RaiderCanvas submission time as your final timestamp
- 10% penalty per day for late submission