OCSP Confessions

Mike Helm
Olle Mulmo
Milan Sova

Quick overview

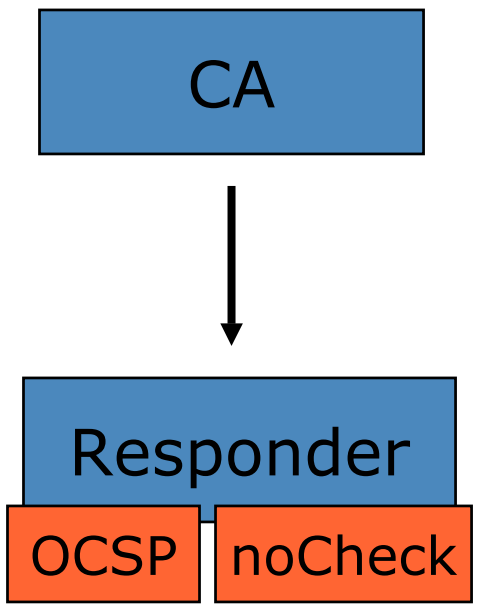
- Online Certificate Status Protocol (RFC2560)
- Lightweight request/response (HTTP)
- Removes burden of CRL distribution and update
- Clients still have to do path validation!

Trust model alternatives

1. CA signs responses
2. Dedicated OCSP signing key certified by CA (extKeyUsage)
3. Other trusted party

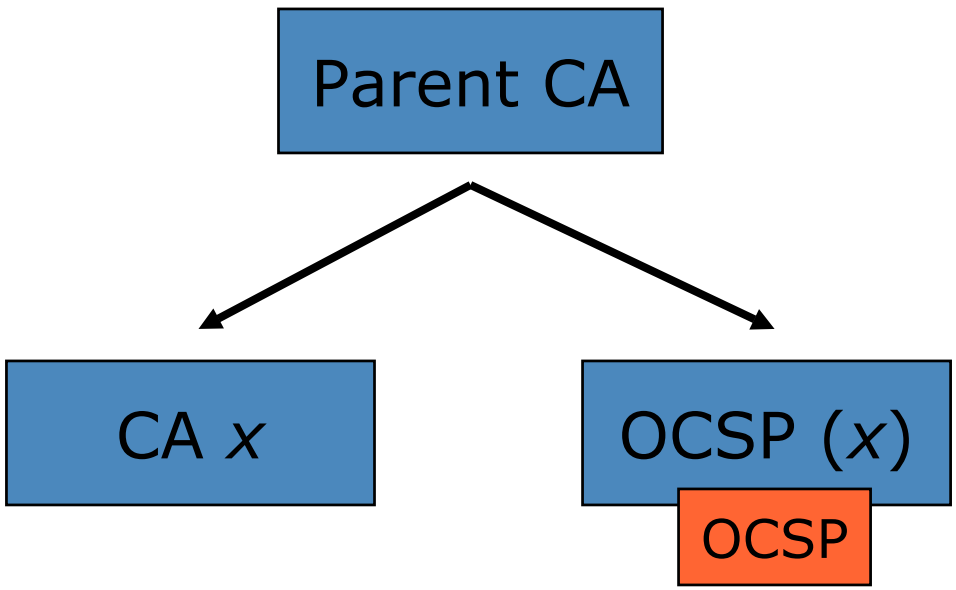
Revocation status of OCSP responder?

- Don’t
- OCSP-no-check extension
- Shortlived signature certificates



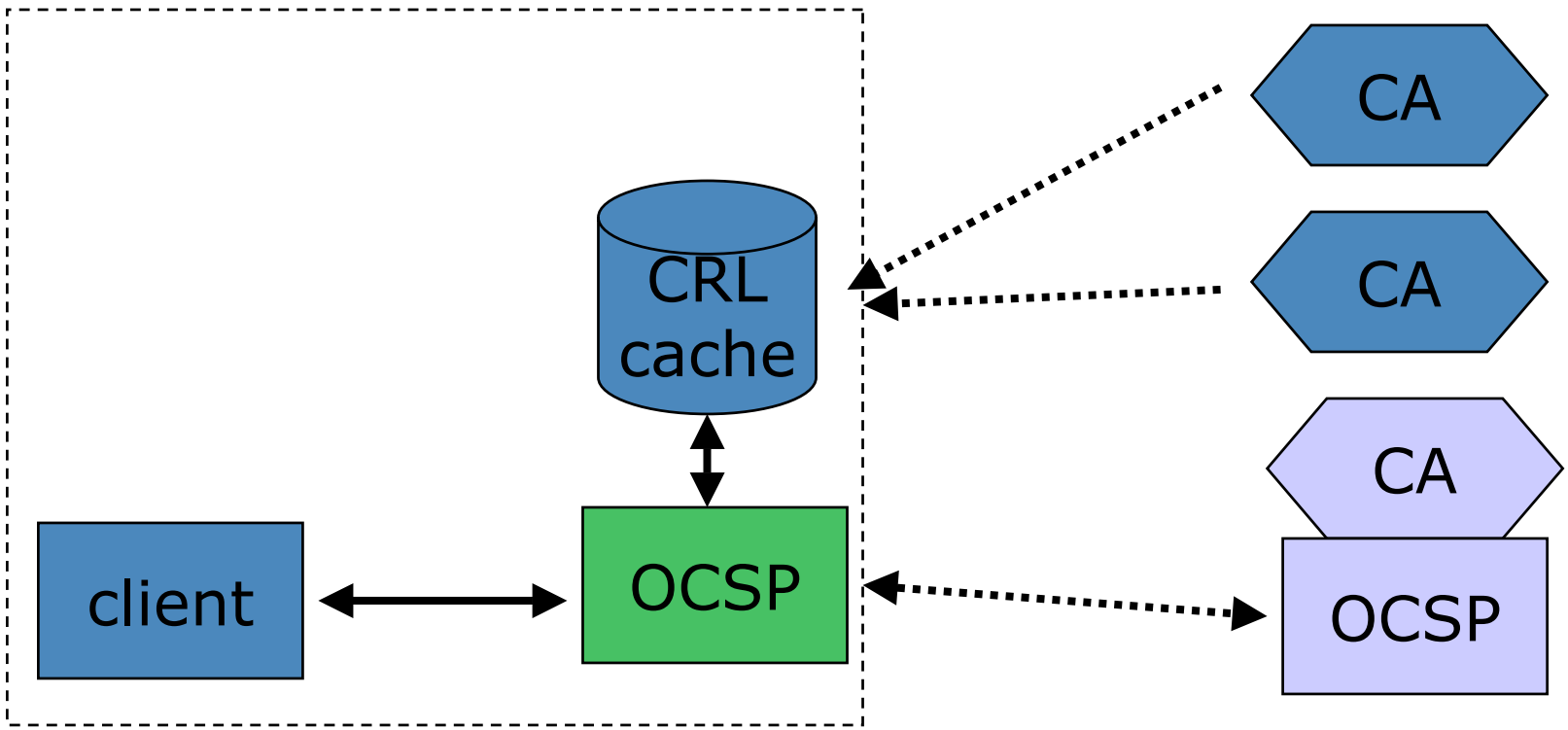
Extended alternative

- Used in some financial sector PKIs
- RFC compliant in an odd kind of way



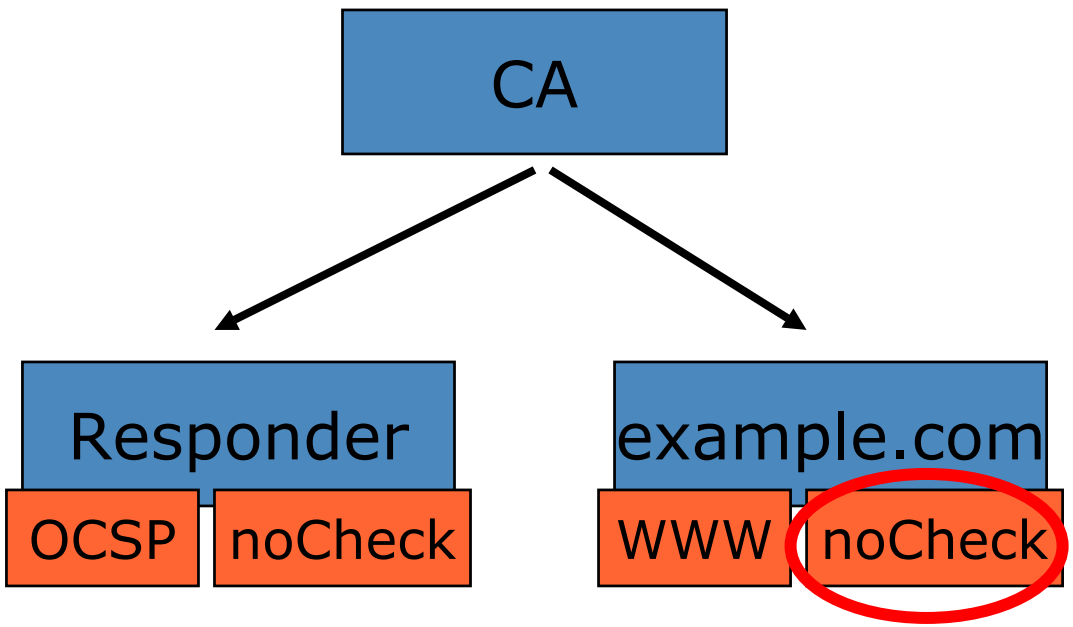
Typical deployment

- Organizational proxy
  - "Other party" model



HTTP or HTTPS?

- Responses are signed
- Error messages are not
- Easy to shoot yourself in the foot…



Document status

- Requirements gathering
- Eliminate some of the options OCSP offers
- Current content: Zip, zero, nada