

ZERTIFIKAT-REVOCAATION MIT OCSP (ALTNERATIVE ZU SPERRLISTEN)

Kein
Prüfungstoff

← → ↻ pki.dfn.de/crl/globalocsp/ ☆ 🔍

OPAL - Online-Platt... Reports to help co... Wie Google Daten... Signal >> Blog >>... GEO information an... Cover Your Tracks

DFN
deutsches forschungnetz

Home | Validierungsdienste (CRL und OCSP) | OCSP Global

- ▶ Überblick DFN-PKI
- ▶ Die CAs im DFN
- ▶ Grid Zertifikate
- ▶ DFN-AAI Zertifikate
- ▶ Zeitstempeldienst
- ▶ Policies
- ▶ Wurzelzertifikate
- ▼ Validierungsdienste (CRL und OCSP)
 - ▶ CRLs Global
 - OCSP Global
 - ▶ CRLs Grid
 - ▶ CRLs Basic
- ▶ FAQ DFN-PKI
- ▶ Kontakt und Support
- ▶ DFN-PKI Blog
- ▶ DFN-Verein

OCSP - Online Certificate Status Protocol

Das OCSP (Online Certificate Status Protocol) ermöglicht es, den Sperrstatus von Zertifikaten online zu prüfen. OCSP ist damit eine Alternative zu den etablierten Sperrlisten (Certificate Revocation List - CRL).

Wie **funktioniert** OCSP?

- Bei jeder Nutzung eines Zertifikats wird eine Anfrage nach dem Sperrstatus des Zertifikats an einen Server (OCSP-Responder) gestellt.
- Wenn die Antwort positiv ist, kann das Zertifikat genutzt werden.

OCSP kann unter folgenden **Voraussetzungen** genutzt werden:

- Es steht ein OCSP-Responder zur Verfügung
- Das Zertifikat (mit dem z.B. ein Webserver geschützt wird) muss OCSP-fähig sein. In der DFN-PKI sind im Sicherheitsniveau "Global" seit 2012 alle Serverzertifikate OCSP-fähig. Nutzerzertifikate in "Global" sind seit Dezember 2014 per Default OCSP-fähig.
- Die Anwendung (z.B. ein Webbrowser) muss OCSP unterstützen

In der DFN-PKI wird ein OCSP-Responder betrieben.

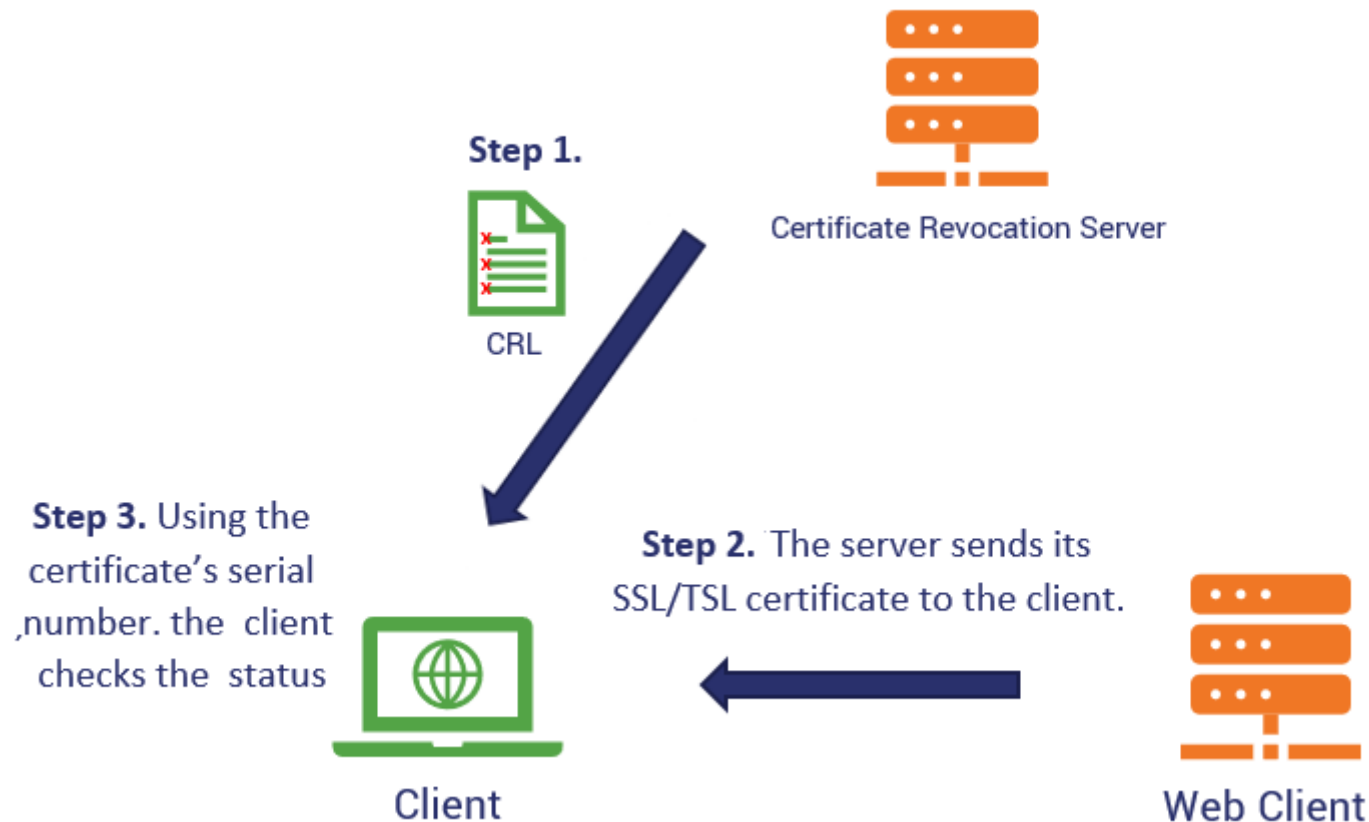
Impressum
Datenschutz

ONLINE CERTIFICATE STATUS PROTOCOL

- Herkömmliche Sperrlisten
 - Client lädt periodisch Sperrliste herunter, entfernt alle gesperrten X.509-Zertifikate aus seinem TrustStore-Repository
 - Funktioniert offline
- OCSP
 - Validierungsdienst erlaubt die Statusabfrage eines Zertifikats in Echtzeit
 - Funktioniert online
- Macht mein Browser OCSP?
 - Ungültiges OCSP-fähiges Zertifikat: <https://revoked-demo.pca.dfn.de/>
 - Gültiges OCSP-fähiges Zertifikat: <https://info.pca.dfn.de/>

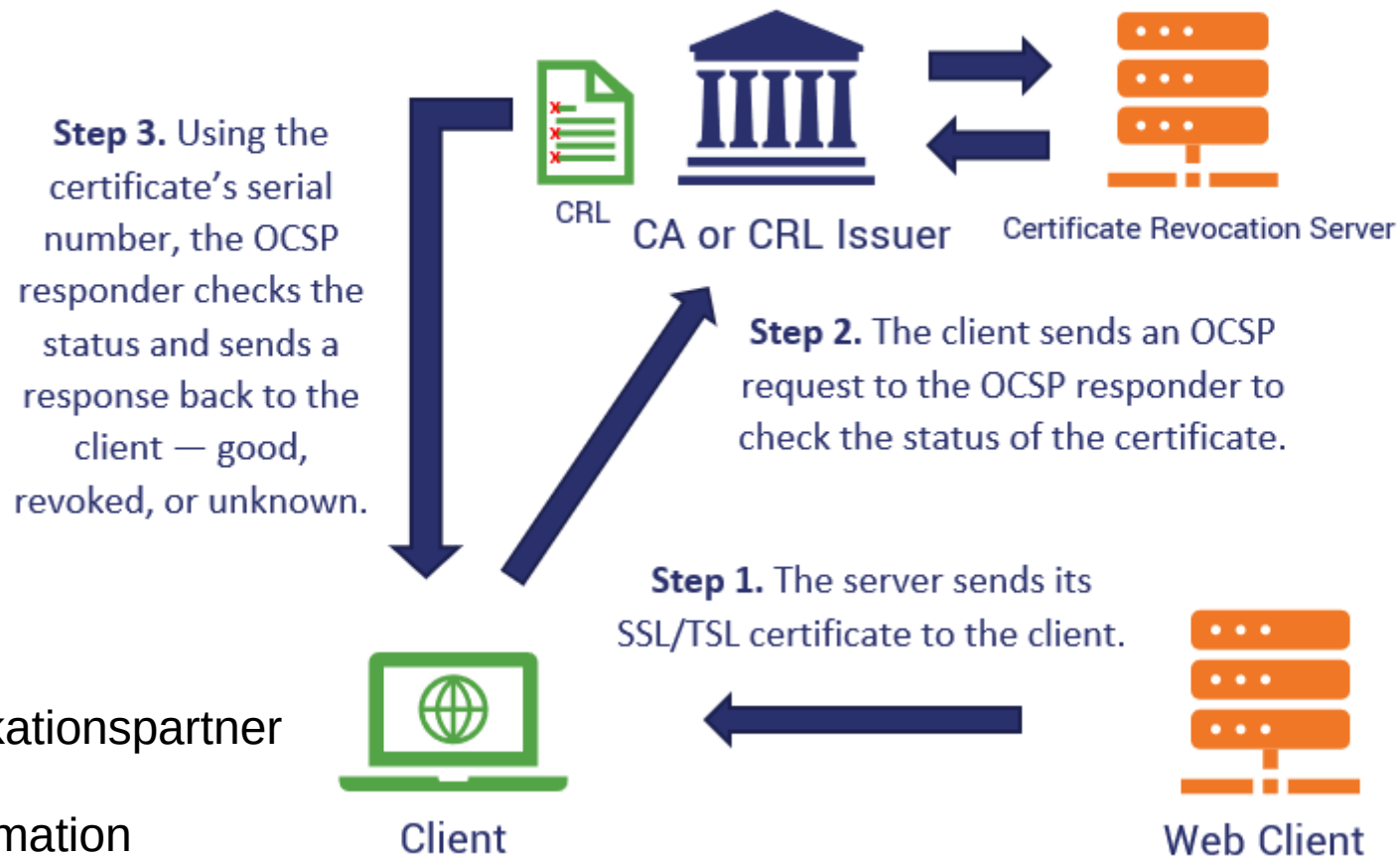
SPERRLISTEN ABLAUF

- Periodischer Abruf der Certificate Revocation List
- Offline-Prüfung vor jeder Verbindung mit einem zertifizierten Server



OCSP ABLAUF

- Online-Prüfung vor jeder Verbindung mit einem zertifizierten Server:

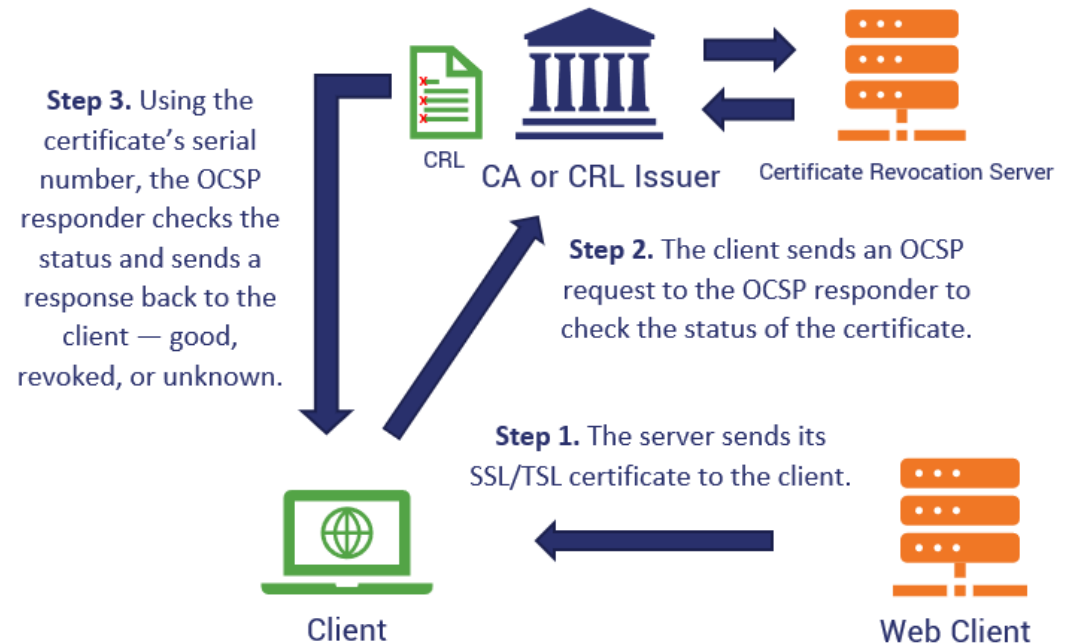


Daten:

- Kommunikationspartner
- Zertifikat
- Sperrinformation
- Metadaten (Uhrzeit, Protokollversion, ...)

OCSP BEWERTUNG

- Parteien
 - OCSP-Client
 - OCSP-Server
- Verbindungen
 - Client→OCSP-Server
 - OCSP-Server→Client
- Services
 - Zertifikat-Validierung
- Daten
 - Kommunikationspartner
 - Zertifikat
 - Sperrinformation
 - Metadaten (Uhrzeit, Protokollversion, ...)

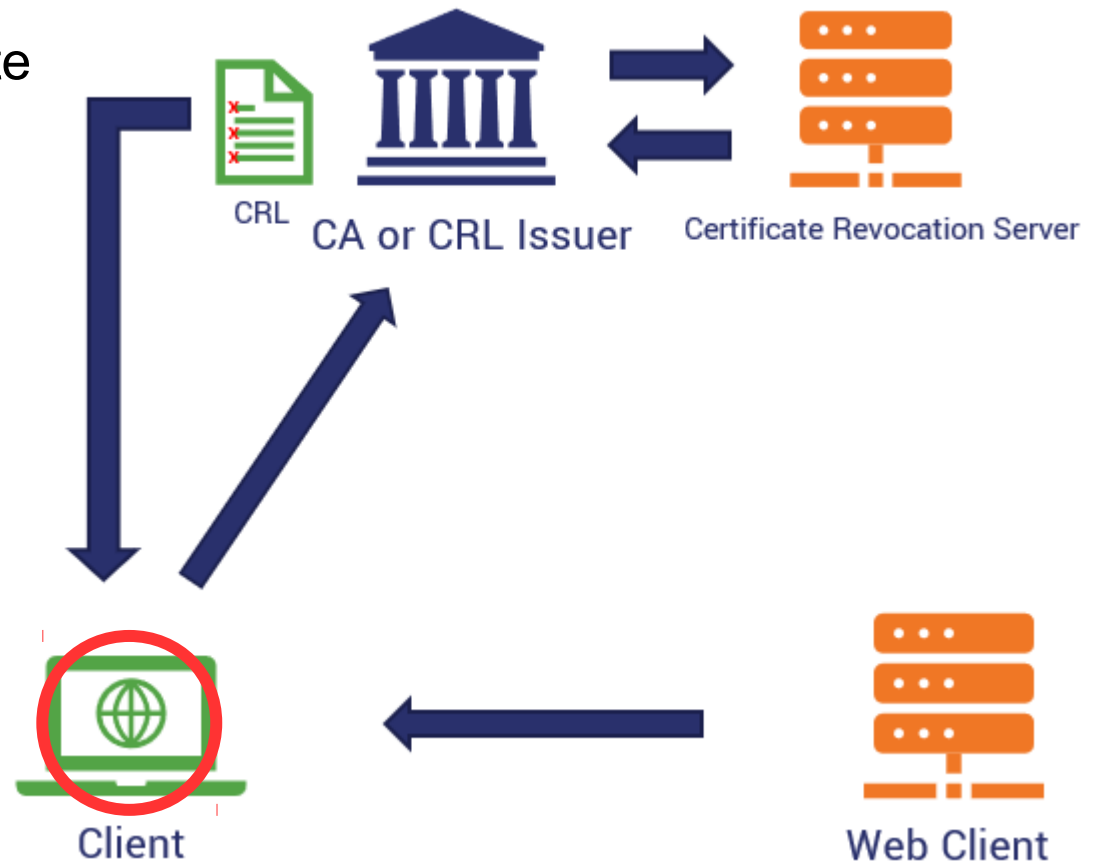


Was passiert, wenn man die Verbindungen, Services, Daten

- unterbricht
- modifiziert
- abfängt
- fälscht

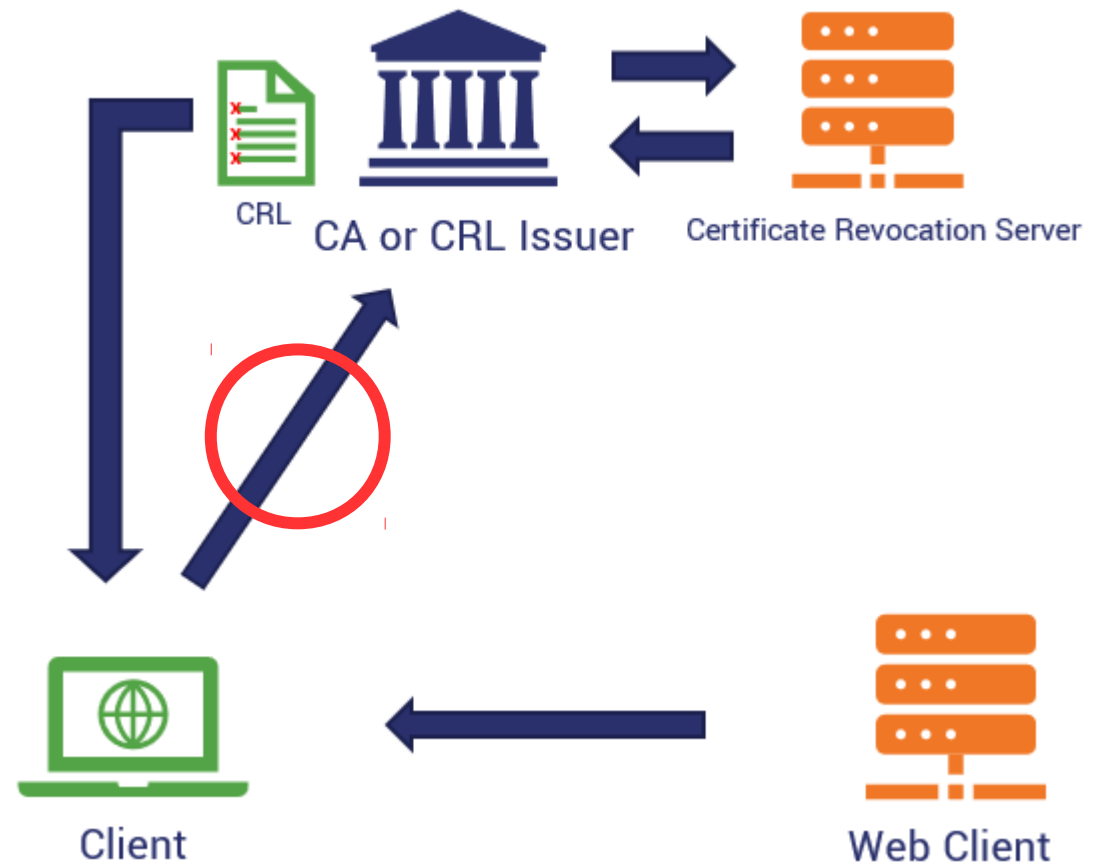
OCSP-CIENT

- Vertraulichkeit
→ Wer ist der vom Client gewählte OCSP-Server?
- Verfügbarkeit
→ unproblematisch
- Integrität
→ Fehlkonfiguration, Trojaner?
- Datenschutz
→ unproblematisch



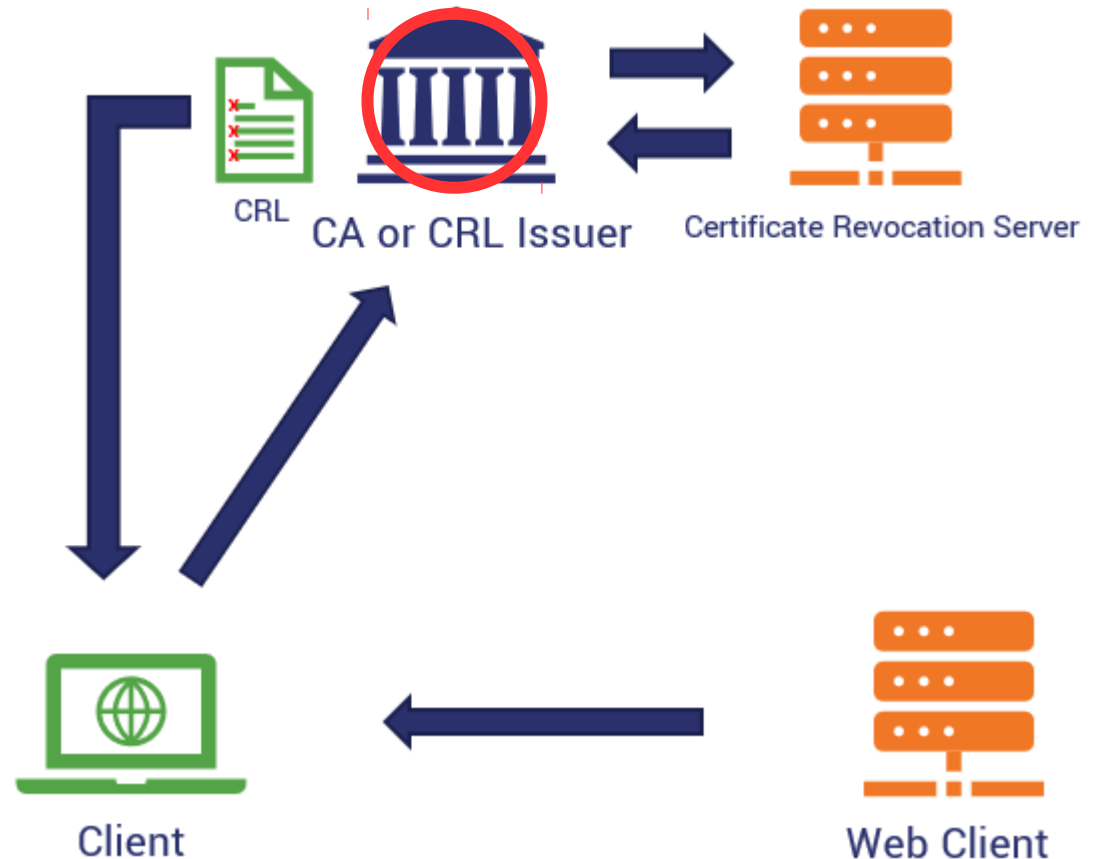
CLIENT → OCSP-SERVER (OCSP REQUEST)

- Vertraulichkeit
→ „Client will Zertifikat prüfen“
- Verfügbarkeit
→ kann unterbrochen werden!
→ Latenz!
- Integrität
→ signiert, TLS-verschlüsselt
- Datenschutz
→ „Client will Zertifikat prüfen“



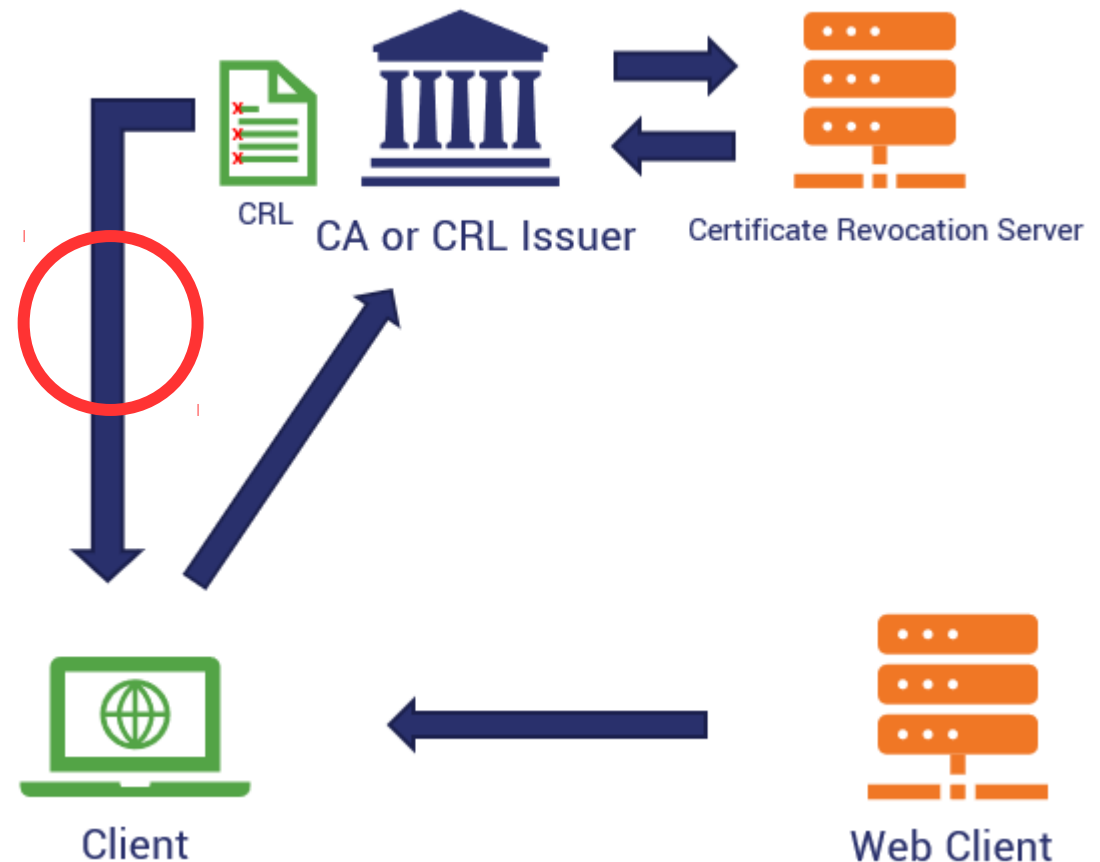
OCSP-SERVICE, OCSP-SERVER

- Vertraulichkeit
→ erfährt, wer mit wem redet
- Verfügbarkeit
→ Single Point of Failure!
→ Latenz! Viele Clients parallel
- Integrität
→ Vertrauen in Revocation List!
- Datenschutz
→ häuft Kommunikationsprofile pro IP-Adresse an!



OCSP-SERVER → CLIENT (OCSP RESPONSE)

- Vertraulichkeit
→ unproblematisch
- Verfügbarkeit
→ kann unterbrochen werden!
→ Latenz!
- Integrität
→ signiert, TLS-verschlüsselt
- Datenschutz
→ unproblematisch



DISKUSSION OCSP

- Pro's
 - Lücke zwischen „Zertifikat wird ungültig“ und „Client lädt CRL herunter und prüft diese offline“ wird kleiner
- Con's
 - Validierungsdienst
 - Single Point of Failure, attraktives Angriffsziel, sammelt Kommunikationsprofile vieler Clients, Latenz hat Auswirkungen auf Clients
 - Kommunikationsverbindungen
 - Können unterbrochen werden, Außenstehende erfahren dass Client OCSP einsetzt (aber nicht den Inhalt der Zertifikate)
 - Client
 - Möglichkeiten zur Fehlkonfiguration, mit Schadcode infiziert?
 - Was tut der Client, wenn der Validierungsdienst nicht antwortet?

LÖSUNGSOPTION: OCSP-STAPLING

- Server fragt selber den OCSP-Validierungsdienst regelmäßig ab
- Server hängt signierte Antwort des Validierungsdienstes beim TLS-Handshake an sein eigenes Zertifikat an
 - Client muss nicht selber den Validierungsdienst fragen
 - Validierungsdienst erfährt nicht, wer mit wem kommuniziert
 - Validierungsdienst muss nicht online sein, keine Performanzprobleme

