OCSP

Inhaltsverzeichnis

OCSP prüft online, ob ein TLS-Zertifikat widerrufen wurde. Clients oder Server fragen einen Responder der CA, statt allein auf periodische CRL-Listen zu setzen.

1 Funktionsweise

Bei der TLS-Prüfung wird der Zertifikatsstatus beim OCSP-Responder erfragt. OCSP Stapling liefert die Antwort direkt vom Server mit und entlastet Clients sowie die CA.

- **Status:** good / revoked / unknown
- **Stapling:** Server reicht signierte OCSP-Antwort weiter
- **CRL-Alternative:** oft frischer und schlanker

2 Typische Einsatzbereiche

- Öffentliche Web- und API-TLS
- Härtung von Zertifikatsvalidierung
- Mail- und interne PKI-Szenarien

3 Wichtige Hinweise

- Erreichbarkeit des Responders beeinflusst UX/Verfügbarkeit.
- Stapling aktivieren und überwachen.
- Soft-Fail vs. Hard-Fail bewusst konfigurieren.

4 Fazit

OCSP macht Widerruf prüfbar – besonders mit Stapling ein wichtiger Baustein moderner TLS-Betriebspraxis.