DANE

Inhaltsverzeichnis

DANE bindet TLS-Zertifikate oder CA-Einschränkungen an DNSSEC-signierte DNS-Records (TLSA). Clients können so Zertifikate unabhängig vom klassischen CA-Ökosystem prüfen.

1 Funktionsweise

In der DNS-Zone liegen TLSA-Records, die erlaubte Zertifikate oder CAs beschreiben. Voraussetzung ist DNSSEC, damit die Records nicht manipulierbar sind.

- **TLSA:** Zertifikats-/CA-Pinning per DNS
- **DNSSEC:** Authentizität der Policy
- **SMTP/TLS-Use-Cases:** u. a. Mail-Transport

2 Typische Einsatzbereiche

- Zusätzliche Absicherung von Mail- und Dienst-TLS
- Pinning ohne App-seitige Hardcodes
- Umgebungen mit DNSSEC-Kompetenz

3 Wichtige Hinweise

- Ohne DNSSEC ist DANE wirkungslos bzw. riskant.
- Key-/Zertifikatswechsel müssen TLSA mitziehen.
- Client-Support ist je nach Ökosystem unterschiedlich.

4 Fazit

DANE verknüpft DNSSEC und TLS – starkes Binding, aber betrieblich nur mit sauberer DNSSEC- und Zertifikatspflege tragfähig.