TLSA-Record

Inhaltsverzeichnis

- 1 Bedeutung des Record-Typs
- 2 Geschichte
- 3 Nutzen und Zweck
- 4 Funktionsweise
- 5 Beispiel
- 6 Fazit

Ein TLSA-Record bindet TLS-Zertifikate kryptografisch an eine Domain oder einen Dienst.

1 Bedeutung des Record-Typs

TLSA steht für **TLS Authentication**. Der Record ist Teil von **DANE** (DNS-based Authentication of Named Entities) und erlaubt es, Zertifikate oder Schlüssel direkt über DNS zu verifizieren.

2 Geschichte

TLSA wurde eingeführt, um das klassische Vertrauen ausschließlich in Zertifizierungsstellen zu ergänzen. Voraussetzung für den sicheren Einsatz ist DNSSEC.

3 Nutzen und Zweck

TLSA-Records erhöhen die Sicherheit von TLS-Verbindungen, indem sie Zertifikatsprüfung über DNS ermöglichen. Besonders relevant ist dies für E-Mail-Dienste (SMTP, IMAP, POP3).

4 Funktionsweise

Der Record enthält Angaben zur Verwendung, zum Selektor, zum Hash-Verfahren sowie zum eigentlichen Hashwert des Zertifikats oder Schlüssels. Clients prüfen diese Informationen zusätzlich zur normalen TLS-Validierung.

5 Beispiel

```
_443._tcp.beispiel-example.de TLSA 3 1 1 abcd1234...
```

6 Fazit

TLSA bietet ein hohes Sicherheitsniveau, setzt jedoch DNSSEC und passende Client-Unterstützung voraus.