DNSSEC

Inhaltsverzeichnis

DNSSEC schützt DNS-Antworten kryptografisch vor Manipulation. Resolver können prüfen, ob Datensätze authentisch und unverändert von der autoritativen Zone stammen.

1 Funktionsweise

Zonen werden mit Schlüsselpaaren signiert. Resolver validieren Signaturen entlang der Vertrauenskette von der Root bis zur Domain.

- **RRSIG/DNSKEY:** Signaturen und Schlüssel
- **DS-Records:** Vertrauensanker zur Parent-Zone
- **Validation:** Resolver markieren Antworten als secure/bogus

2 Typische Einsatzbereiche

- Schutz vor Cache Poisoning und gefälschten DNS-Antworten
- Voraussetzung für Features wie DANE
- Absicherung kritischer Domains und Mail-Infrastruktur

3 Wichtige Hinweise

- Schlüsselrotation und DS-Updates müssen geplant sein.
- Fehlerhafte DNSSEC-Konfiguration macht Domains unerreichbar.
- Validierende Resolver und korrekte Uhren sind wichtig.

4 Fazit

DNSSEC macht DNS vertrauenswürdiger: Antworten werden prüfbar – mit spürbarem Betriebsaufwand bei Keys und Delegations.