RPKI

Inhaltsverzeichnis

RPKI sichert BGP-Announcements kryptografisch ab: Netzbetreiber attestieren, welche ASN welche Präfixe ankündigen darf. Validatoren erkennen ungültige Routen.

1 Funktionsweise

Prefix-Inhaber erstellen Route Origin Authorizations (ROAs). Router oder Validatoren prüfen eingehende BGP-Updates gegen diese Attestierungen.

- **ROA:** Präfix ? erlaubte Origin-ASN
- **Validation:** valid / invalid / not found
- **Policy:** invalid Routes ablehnen oder bestrafen

2 Typische Einsatzbereiche

- ISP- und Enterprise-BGP-Sicherheit
- Schutz vor versehentlichen und bösartigen Hijacks
- Hardening von Internet-Upstreams

3 Wichtige Hinweise

- Falsche ROAs können eigene Erreichbarkeit spoilern.
- Einführung schrittweise und monitoring-basiert.
- RPKI ersetzt nicht Prefix-Filter komplett.

4 Fazit

RPKI macht Origin-Validation im Internet-Routing möglich – ein wichtiger Schutz gegen BGP-Hijacking und Fehlankündigungen.