



RPKI & Route Origin Authorisations (ROA)

Schutz vor nicht autorisierter Umleitung von Datenverkehr



Stand: 22.03.2023, BETA

Management Summary

Das Internet funktioniert als Zusammenschluss unabhängiger Betreiber, die einander Netze bekannt geben und Datenströme zuleiten. Die Legitimität einer solchen Bekanntgabe wurde erst mit

Einführung von RPKI verifizierbar. Damit wird eine versehentliche oder gezielte Umleitungen des für Ihren OZG Dienst bestimmten Datenverkehrs erschwert.

Ressourcenabschätzung

-  Mittel (50 PT)
-  Ohne neue Hardware

Erläuterung für OZG-Dienstverantwortliche

Bei RPKI werden die zulässigen Betreiber von IP-Netzen durch den Inhaber des IP-Adressblocks benannt. So wird die Kommunikation der Bürgerinnen und Bürgern und Ihrem OZG Dienst gegen missbräuchliche Umleitung geschützt und die Resilienz Ihres OZG Dienstes erhöht. Die Wegeführung (Routing) der Daten im Internet zu Ihrem Dienst ist ohne RPKI anfällig für Manipulationen. Durch

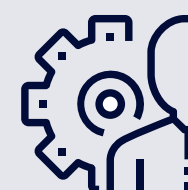
die kryptografische Verknüpfung von IP-Adressblöcken mit der Kennung von Netzbetreibern (ASN) wird die legitime Nutzung durch Zertifikate nachgewiesen. Der Einsatz von RPKI wird vom BSI für Betreiber empfohlen und kann in Deutschland bei der zuständigen regionalen Internet-Registrierungsstelle RIPE NCC vergleichsweise leicht eingerichtet werden.

Referenz



RFC 8659
BSI-CS 118
RIPE NCC 751

Umsetzung



RZ-Betrieb

Technischer Umsetzungsansatz

Durch RPKI bestätigt der legitime Besitzer eines IP-Adressblocks die Verknüpfung mit ASNs durch Zertifikate kryptografisch nachweisbar. Aktuell wird RPKI i. d. R. als „hosted RPKI“ bei der RIPE NCC betrieben. LIRs erhalten hier ein Ressourcenzertifikat, in dem ihre Internet-Ressourcen (Autonomous System Nummern (ASN) IPv4- und IPv6-Präfixe) aufgeführt sind. Mit diesem Zertifikat werden wiederum Route Origin Authorisations (ROA)

signiert. Eine ROA ist ein kryptografisch signiertes Objekt in der RIPE-DB, das Auskunft darüber gibt, welches autonome System (AS) autorisiert ist, ein bestimmtes IP-Präfix zu annonciieren. Die eigentliche Umsetzung muss durch die jeweilige LIR erfolgen, bei der der IP-Adressraum des OZG-Dienstes registriert ist. Das „How-To: RPKI“ des BSI (BSI-CS 118) beschreibt dies detailliert.

ROA in der RIPE Datenbank:

- ROA Name
- AS Number (ASN)
- Gültigkeitszeitraum
- Eine/ mehrere IP-Adressen (CDIR Block sowie maximale Länge)
- RPKI Signatur

Aufbau eines ROA