RPKI (Resource Public Key Infrastructure)

RPKI řeší jeden z největších bezpečnostních problémů internetu: fakt, že protokol BGP je postaven na vzájemné důvěře. Bez RPKI může v podstatě jakýkoliv operátor prohlásit, že „vlastní“ IP adresy někoho jiného, což vede k incidentům známým jako **BGP Hijacking**.

RPKI vytváří hierarchický systém digitálních certifikátů, který propojuje IP adresy s jejich legitimními vlastníky.

Jak RPKI funguje?

Systém se skládá ze tří hlavních pilířů:

1. ROA (Route Origin Authorization)

Vlastník IP adres (např. firma nebo ISP) vytvoří digitálně podepsaný objekt zvaný **ROA**. Tento dokument obsahuje tři klíčové informace:

- Který **autonomní systém** (ASN) smí adresy oznamovat.
- Jaký **prefix** (rozsah adres) se oznamuje.
- **Maximální délku** prefixu (např. zda lze rozsah /24 dále dělit).

2. Repository (Úložiště)

Digitálně podepsané ROA záznamy jsou uloženy v globálních databázích spravovaných regionálními internetovými registry (RIR), jako je například **RIPE NCC** pro Evropu.

3. Route Origin Validation (ROV)

Routery ostatních operátorů si tyto záznamy stahují (obvykle skrze pomocný software zvaný „Validator“) a porovnávají je s tím, co vidí v protokolu BGP.

Stavy validace BGP tras

Když router přijme informaci o trase přes BGP a má zapnuté RPKI, vyhodnotí ji do jednoho ze tří stavů:

Stav	Význam	Akce routeru
Valid	Trasa přesně odpovídá podepsanému záznamu ROA.	Trasa je přijata jako bezpečná.
Invalid	Existuje ROA pro tyto adresy, ale hlásí je jiný AS, nebo je prefix moc dlouhý.	Router trasu obvykle zahodí (ochrana před hijackingem).
Not Found	Pro tyto adresy neexistuje žádný záznam ROA.	Trasa je přijata (aby internet stále fungoval pro ty, co RPKI nemají).

Proč je RPKI důležité?

- **Prevence BGP Hijackingu:** Zabraňuje útočníkům nebo chybně nakonfigurovaným routerům přesměrovat cizí provoz k sobě (např. krádeže kryptoměn přes falešné DNS bank).
- **Prevence Route Leaks:** Pomáhá omezit šíření chyb v konfiguraci, kdy se lokální trasy omylem dostanou do globálního internetu.
- **Důvěryhodnost sítě:** Operátoři, kteří používají RPKI, zvyšují stabilitu a bezpečnost celého globálního internetu.

Omezení RPKI

RPKI řeší pouze to, **kdo** může začít trasu oznamovat (Origin). Neřeší však, zda je cesta k tomuto cíli (seznam AS v BGP) pravdivá. K plnému zabezpečení cesty je potřeba další protokol, jako je **BGPsec**, který je však v praxi mnohem náročnější na implementaci a zatím se příliš nepoužívá.

Související pojmy: BGP, Autonomní systém (AS), IP adresa, BGP Hijacking, RIPE NCC, Digitální podpis.