

# Understanding RPKI

Resource Public Key Infrastructure

April 2021  
Version 2.2

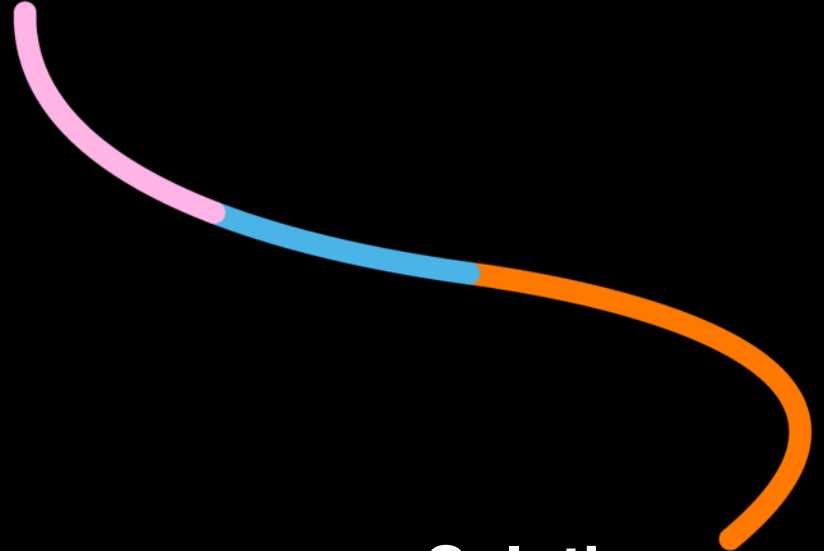
International Carriers



# Agenda

1. What is RPKI ?
2. Why RPKI?
3. ROA: a customer protects itself and the others
4. How does RPKI work ?
5. RPKI validation & filtering workflow
6. What do I have to do ?
7. Use Cases

Techno






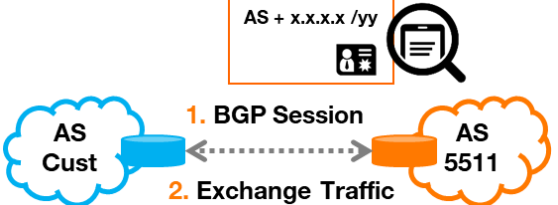
Solutions

# What is RPKI ? - Resource Public Key Infrastructure

**Resource Public Key Infrastructure (RPKI)** is a cryptographic method of signing records (ROA) that associate a **BGP route advertisement** with the intended originating **AS number**

RPKI is a certification-based model to validate that the customer is who it claims to be:

-  This is me (Operator)
  -  This is my network (AS Number and BGP routes)
  -  This signed certificate, called Route Origin Authorization (ROA) proves it... and you can verify it.
- ROAs are distributed by Regional Internet Registries
- Network operators can take routing decisions based on the ROA data: “this prefix is **Valid**, **Unknown** or **Invalid**”



# Stronger

# Strong

# **Why RPKI ? – Secures the Internet routing table, reduces the risk of accidental BGP routing incidents and prevents hijacks**

- **The Internet consists of a number of functionally independent AS which use BGP to exchange routing information in order to exchange traffic**
- **Connectivity and routing topologies are subject to change, which easily propagate globally within a few minutes.**
- **One weakness of this system is that these changes cannot be validated against information existing outside of the BGP protocol itself**
- **RPKI is a way to define an out-of-band (external) system such that the information that are exchanged by BGP can be validated to be correct.**
- **The RPKI standards were developed by the IETF (Internet Engineering Task Force) to describe some of the resources of the Internet's routing and addressing scheme in a cryptographic system.**
- **These information are public, and anyone can get access to validate their integrity using cryptographic methods.**

## **Route Origin Authorization** - When a customer certifies its technical information (AS number and BGP advertisements) by creating ROAs, it protects itself and the rest of the Internet

- **If there is a BGP misconfiguration on the customer side (BGP advertisements not corresponding to a ROA), IP Transit Providers having deployed RPKI will block these invalid BGP advertisements and lower the risk of a global Internet outage.**
- **If a third party unintentionally advertises BGP prefixes belonging to an IP Transit customer, RPKI will avoid Internet routing issues if the customer has had created ROAs for its routes.**
- **If a customer experiences a IP address hijacking (a third party intentionally advertises IP space belonging to the customer), RPKI will avoid traffic to be redirected to the malicious player if the customer has created ROAs for the hijacked prefixes.**

# How does RPKI work ? – ROA and RPKI validation & filtering

Two conditions are required to make the Internet safer

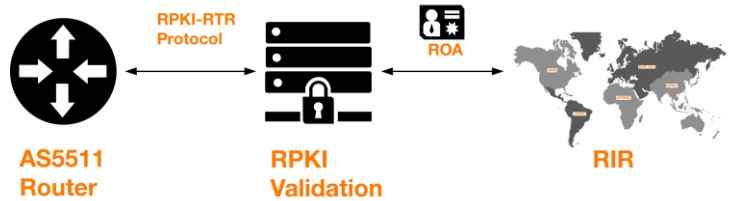
## 1 Create and manage Route Origination Authorization

- Internet players should create and maintain a valid ROA for each set of prefixes it is legitimately authorized and intends to originate
- ROAs are distributed (mostly) from Regional Internet Registries (RIRs) repositories



## 2 Implement RPKI validation & filtering

- Network operators will take BGP routing decisions (filtering) based on ROA information (validation)
- BGP Prefix Status: **VALID**, **INVALID** & **UNKNOWN**

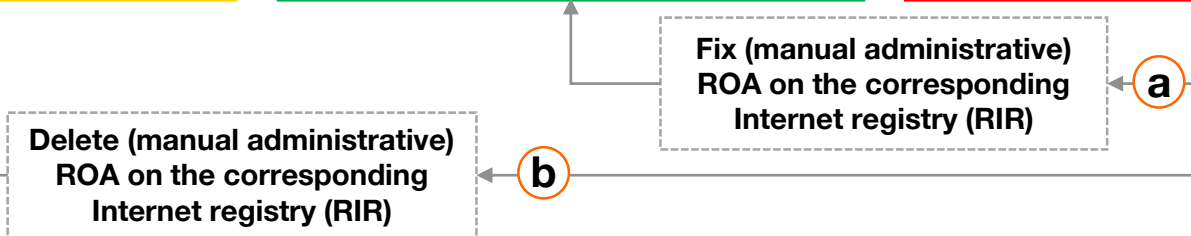
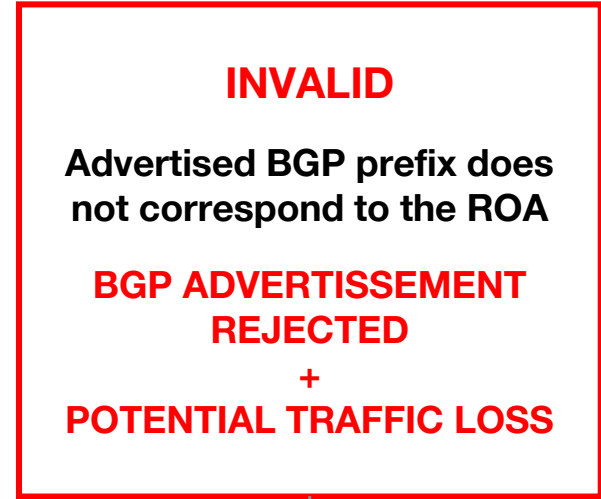


# RPKI validation & filtering workflow

**1** Customers not having created certificates (ROA) for IP prefixes



**2** Customers having adopted RPKI by creating certificates (ROA) for each set of IP prefixes



# What do I have to do to avoid any business impact ?

- 1** It is **mandatory to correct potential data inconsistency in my ROAs** in order to avoid traffic impact. Orange will help me identify problematic IP prefixes.
- 2** I am **highly encouraged** to ensure my **IP space is protected by ROAs**. This will protect my business, and the Internet, from hijacking attempts and/or some routing incidents.
- 3** Before applying any change to the **BGP** architecture in your network, make sure there is consistency between **BGP** advertisements and **Route Origin Authorizations**
- 4** I **might want to deploy RPKI** validation and filtering in my network, it is not mandatory, but it adds an additional level of security to my network and my customers.



# Customer Case 1 – I have **VALID** BGP Prefixes, great news ! Good work!

- **RPKI-based ROV verifies the consistency between ROAs and the BGP prefix information being advertised from your AS to AS5511**
- **VALID BGP Prefixes**
  - BGP prefix + originating AS match the ROA data.
  - Prefix length is less or equal than ROA's maximum length.
- **Customer prefixes covered by a ROA are protected against “Route Hijacks”**
  - “Route Hijack” occurs when an AS advertises prefixes that have not been assigned to it. It usually are malicious attempt. The attacker objective is to reroute traffic in order to intercept or modify traffic.
- **Issuing ROAs allows to increase Internet security and stability.**
- **If changes are made on the BGP architecture, make sure to update the ROA corresponding parameter.**
  - For example: prefix length update

# Customer Case 2 – I have **INVALID** BGP Prefixes – Oh, no!

- **RPKI-based ROV verifies the consistency between ROAs and the BGP prefix information being advertised from your AS to AS5511**
- **INVALID BGP Prefixes**
  - BGP prefix + originating AS does not match the ROA data (IP space, ASN or Max Length)
  - BGP prefixes advertisement will be rejected !
  - Traffic towards the corresponding prefixes will be lost unless an alternate route exists in the routing table.
- **Customer with INVALID BGP prefixes must log into the corresponding RIR and cleanup the issue by updating the ROA**
  - Once the cleaning is done, the BGP Prefixes status will become **VALID** (or **UNKNOWN** if the ROA is deleted)

# Customer Case 3 – I have UNKNOWN BGP Prefixes... Oh bummer !

- RPKI-based ROV verifies the consistency between ROAs and the BGP prefix information being advertised from your AS to AS5511
- **UNKNOWN BGP Prefixes**
  - No ROA exists, hence the BGP prefix is assigned the **UNKWONWN** status
- Customer prefixes with an **UNKWONWN** RPKI state are de facto unprotected against “Route Hijacks”
- There is no traffic impact towards **UNKWONWN** BGP prefixes.

# Thank you



**Engage**  
**2025**

