

Considerations on Authoritative Information for Source Address Validation

Authors: **Lancheng Qin** (Zhongguancun Lab)
Dan Li (Tsinghua University)

March, 2026

Introduction

- SAV and Authoritative Information

- ◆ SAV relies on authoritative information to determine which source addresses are legitimate.
- ◆ However, problems may arise when using such information

- This document provides a conceptual framework for understanding authoritative information in the context of SAVNET, including:

- ◆ What constitutes authoritative information and which sources can be trusted
- ◆ How to handle missing authoritative information
- ◆ How to reconcile conflicting authoritative sources
- ◆ The role of non-authoritative information as a reference in contextual or policy-based decisions

What constitutes authoritative information

- To be considered authoritative, information should meet the following criteria:
 - ◆ Organizational authority: Maintained by an entity with authority over the relevant prefixes or networks
 - ◆ Verifiability : Authenticity can be verified (e.g., cryptographic validation)
 - ◆ Timeliness: Reflects current operational state and is updated promptly
 - ◆ Integrity and security: Resistant to unauthorized modification or tampering

- Typical Authoritative Sources in SAVNET
 - ◆ RPKI objects: ROAs, ASPAs, TOAs providing explicit origin or transit authorization
 - ◆ Local / static configuration: Operator-defined rules for hosts, non-BGP customer networks, or external ASes

- Note on Authoritative Information
 - ◆ May occasionally be incorrect or stale (e.g., authority forgets to update)
 - ◆ Sadly, it is difficult or even impossible for SAV to verify correctness of authoritative information

How to handle missing authoritative information

- Problem: SAV may lack authoritative information for some prefixes or source entities, e.g.,:
 - ◆ No relevant RPKI objects (ROAs, ASPAs, TOAs) exist
 - ◆ Local operator configuration is not defined
- Possible approaches to handle traffic sourced from such prefixes
 - ◆ Conservative: Block traffic by default → safe, but may drop legitimate packets
 - ◆ Permissive: Allow traffic by default → avoids disruption, but may accept spoofed packets
 - ◆ Contextual: Use non-authoritative information → enables incremental deployment
 - ◆ Intermediate Actions: Permit + log, rate-limit, redirect, monitor [I-D.ietf-savnet-general-sav-capabilities]
- Note on non-authoritative information (e.g., route data, IRR data)
 - ◆ May be incorrect or stale
 - ◆ Should be validated before using for SAV enforcement

How to reconcile conflicting authoritative sources

- Problem: Multiple authoritative sources may provide conflicting statements, e.g.,
 - ◆ RPKI objects conflicts for the same prefix
 - ◆ Local/static configuration conflicts with other authoritative sources

- Principle
 - ◆ Treat all authoritative sources as equally credible
 - ◆ Non-authoritative information may be consulted as a reference to support operational understanding, but it cannot override authoritative information

Next Step

- This draft is in a primary stage and future work is needed:
 - ◆ Refine authoritative attributes and sources
 - ◆ Detail principles for using authoritative vs non-authoritative information
 - ◆ Explore how SAV authoritative information can be registered and maintained at authoritative sources, as well as how such information can be coordinated across different authoritative sources
 - ◆ Any other suggestions?

- Comments and Collaboration are welcome to improve the draft

Thanks