TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

The Importance of Route Origin Authorization

nog.fi Seminar 16.11.2022

Ossi Kuosmanen
Senior Specialist, CERT-FI

CERT-FI works to prevent information security incidents and disseminates information on information security matters

TRAFICOM

8.11.2022

CERT-FI’s take on Routing (BGP) Security?

CERT-FI

- Computer Emergency Response Team
- The duties of CERT-FI include:
  - **preventing information security violations**
  - disseminating information about information security matters.
- The objective of CERT-FI's activities is to:
  - **ensure the proper and safe functioning of public communications networks and services**
  - **protect the vital functions of society.**
- Our CERT services provide help in information security matters. In addition to general awareness about information security, we can also assist in the technical investigation of severe information security violations.
- Contact us at cert@traficom.fi
- Report incidents to us: https://www.kyberturvallisuuskeskus.fi/en/report

ENISA - 7 Steps to shore up the Border Gateway Protocol (BGP)

- We encourage electronic communications providers and other organizations running an Autonomous System (AS) to implement these 7 measures as a *minimum* (published 2019):
  1. BGP Monitoring & Routing Anomaly Detection
  2. BGP Coordination
  3. Prefix Filtering
  4. BGP AS Path Filtering
  5. Bogon Filtering
  6. TTL Security (GTSM)
  7. RPKI

MANRS - Network Operator Actions

- These **C**ompulsory and **R**ecommended actions are based on well-established industry best practices and have been selected on the basis of an assessment of the balance between small, incremental costs to individual network operators and the potential common benefits:
  1. Prevent propagation of incorrect routing information (**C**)
  2. Prevent traffic with spoofed source IP addresses – Filtering (**R**)
  3. Facilitate global operational communication and coordination (**C**)
  4. Facilitate routing information on a global scale – IRR (**C**)
  5. Facilitate routing information on a global scale – RPKI (**R**)

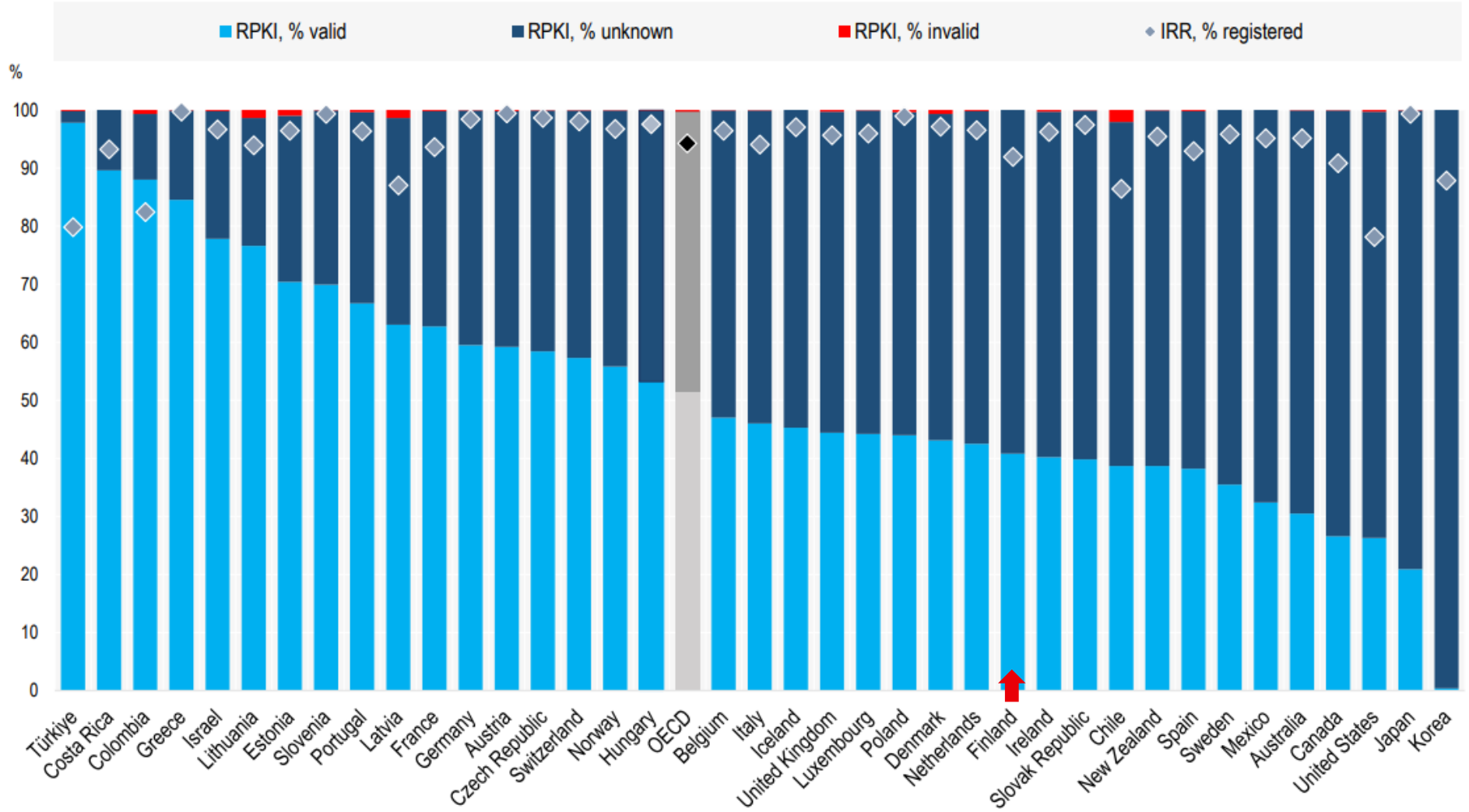
MANRS - The IXP Program Action Set

IXP must demonstrate commitment by implementing all **M**andatory and at least one **A**dditional IXP Program Actions:

1. Prevent propagation of incorrect routing information. (**M**)
2. Promote MANRS to the IXP membership. (**M**)
3. Protect the peering platform. (**A**)
4. Facilitate global operational communication and coordination between network operators. (**A**)
5. Provide monitoring and debugging tools to the members. (**A**)

The current state of RPKI adoption in Finland

IRR and RPKI adoption, OECD countries (June 2022)

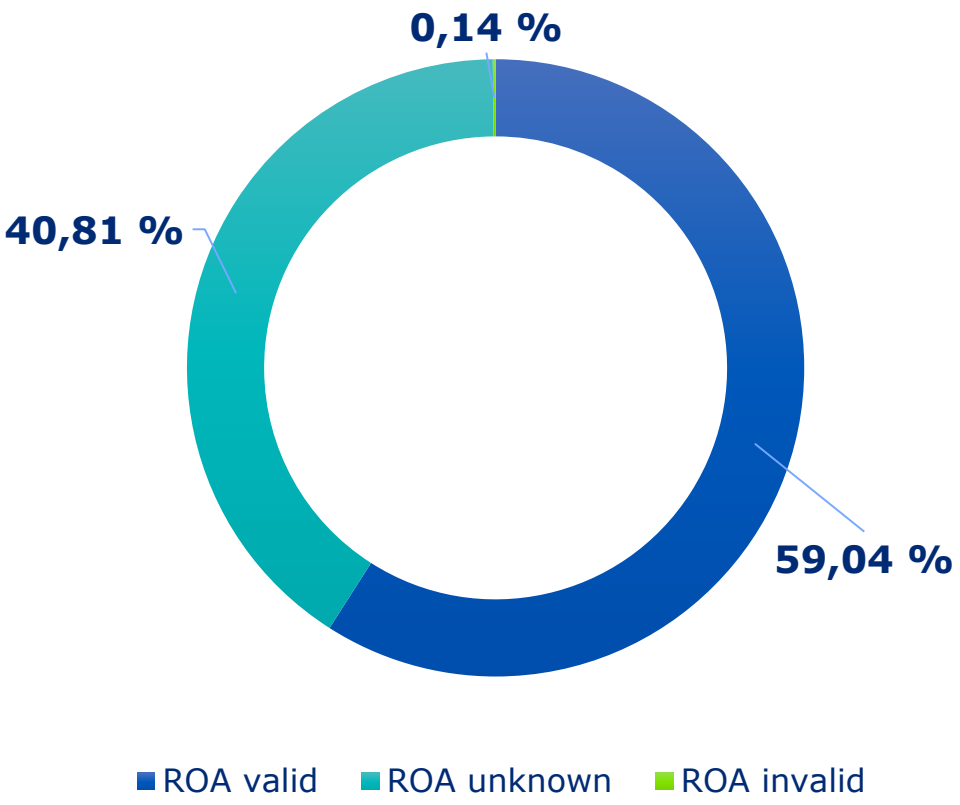


Source: OECD (2022), "Routing security: BGP incidents, mitigation techniques and policy actions", https://doi.org/10.1787/40be69c8-en.

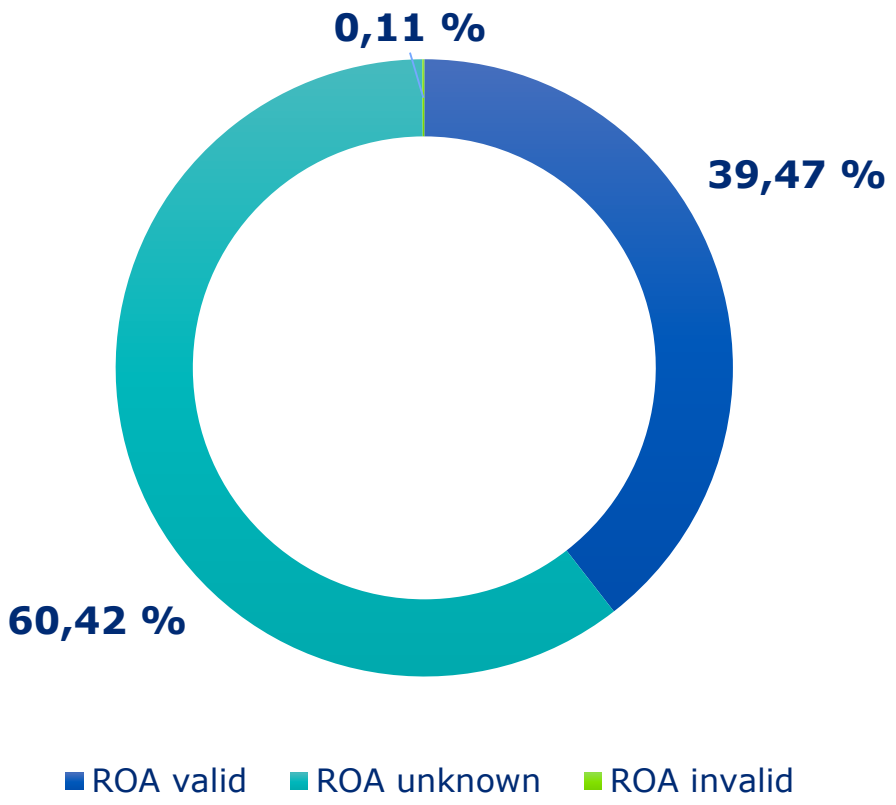
Source:
RIPEstat RPKI check
Query time:
2022-11-08 08:00 UTC

RPKI ROA Adoption - Ficix members

Routes All



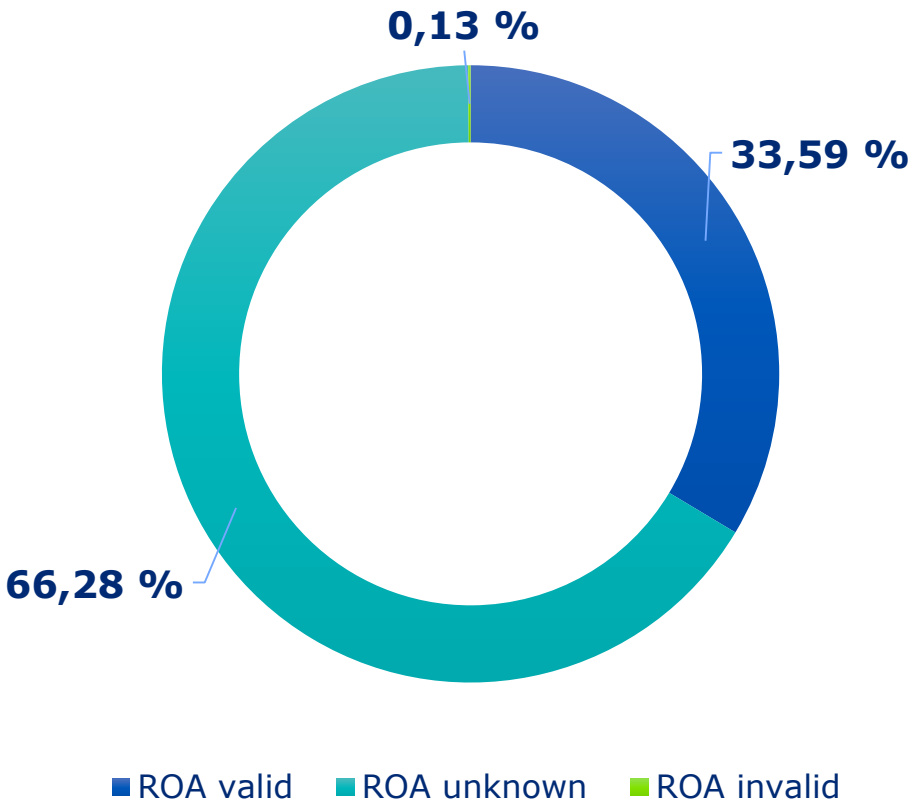
Routes ”FI”



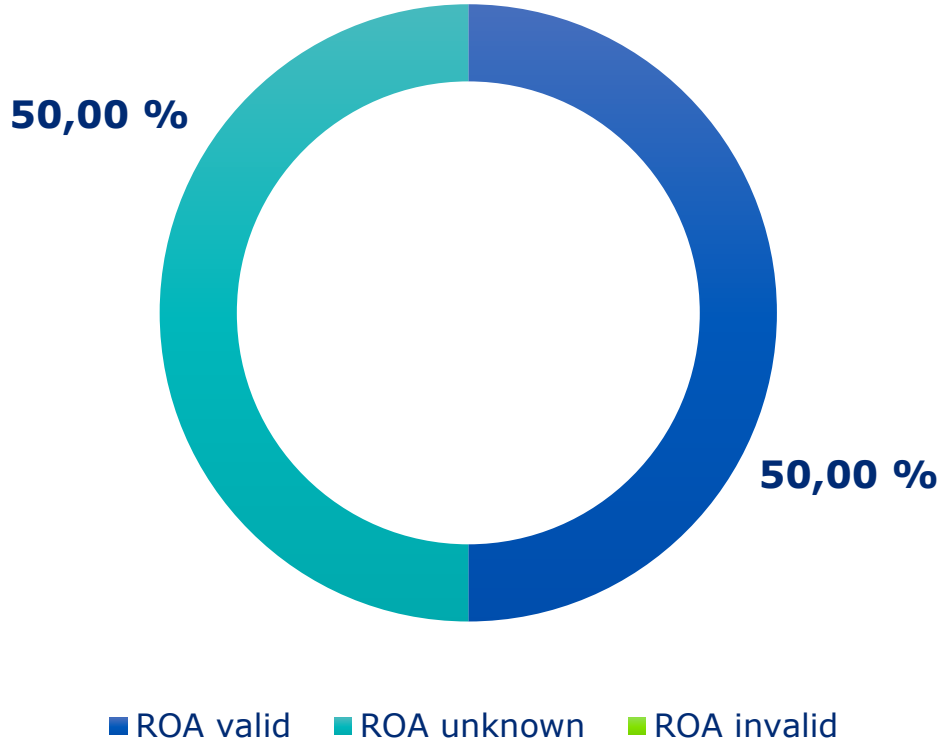
Source:
RIPEstat RPKI check
Query time:
2022-11-08 08:00 UTC

RPKI ROA Adoption - TREX members

Routes All

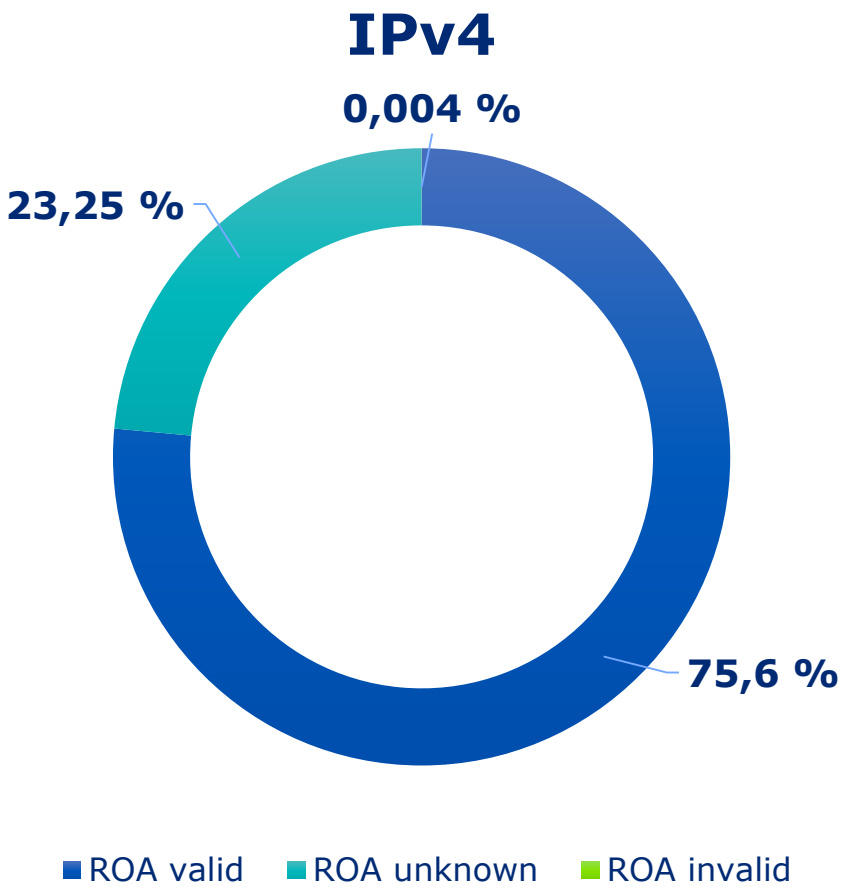


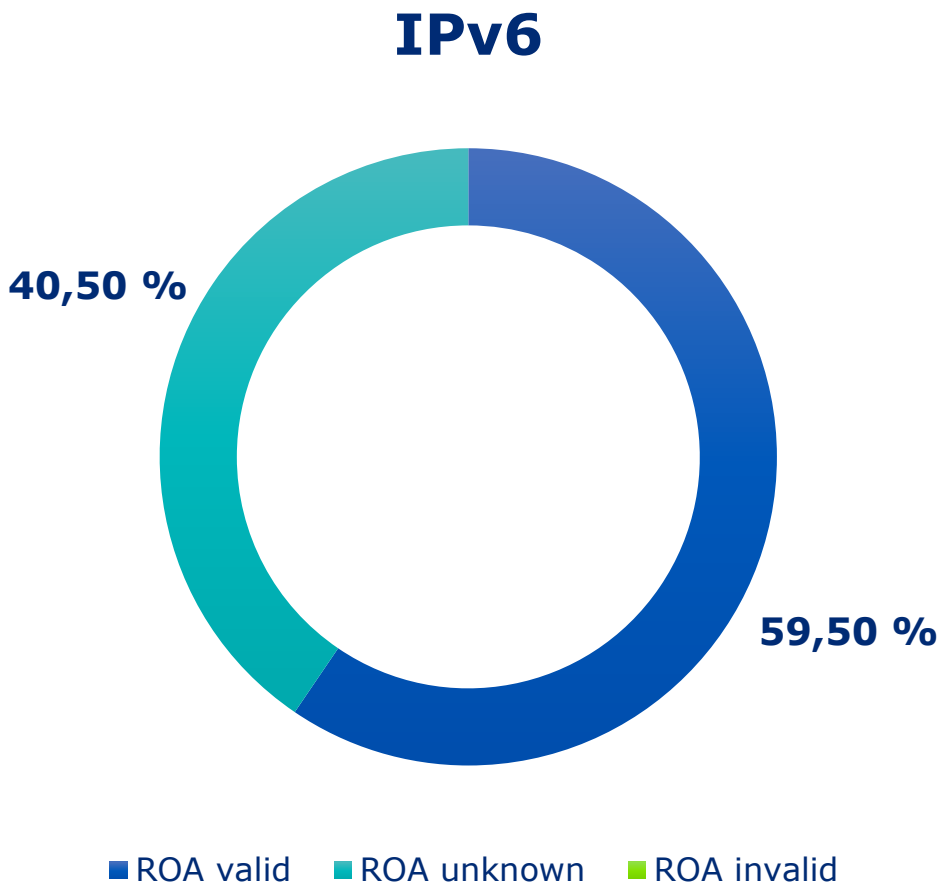
Routes ”FI”



Source:
RIPEstat RPKI check
Query time:
2022-11-08 08:00 UTC

RPKI ROA Adoption - FI Address space

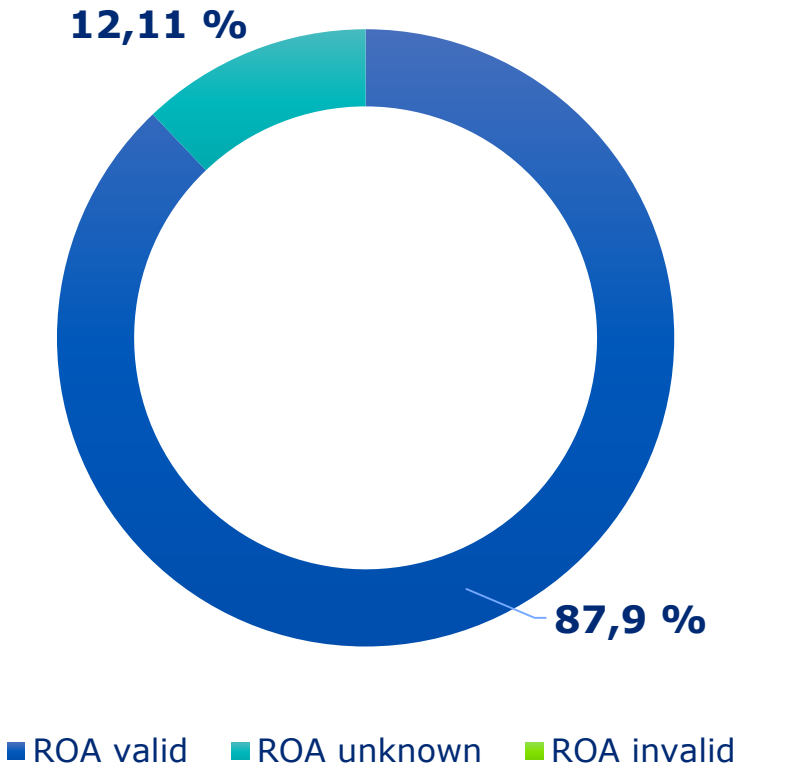




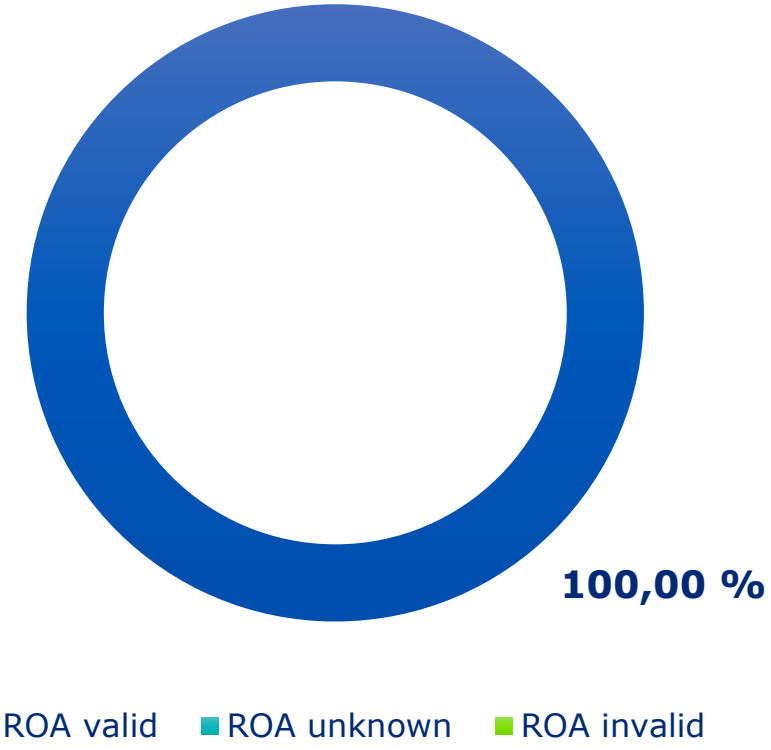
Source:
RIPEstat RPKI check
Query time:
2022-11-08 08:00 UTC

RPKI ROA Adoption - AX Address space

IPv4

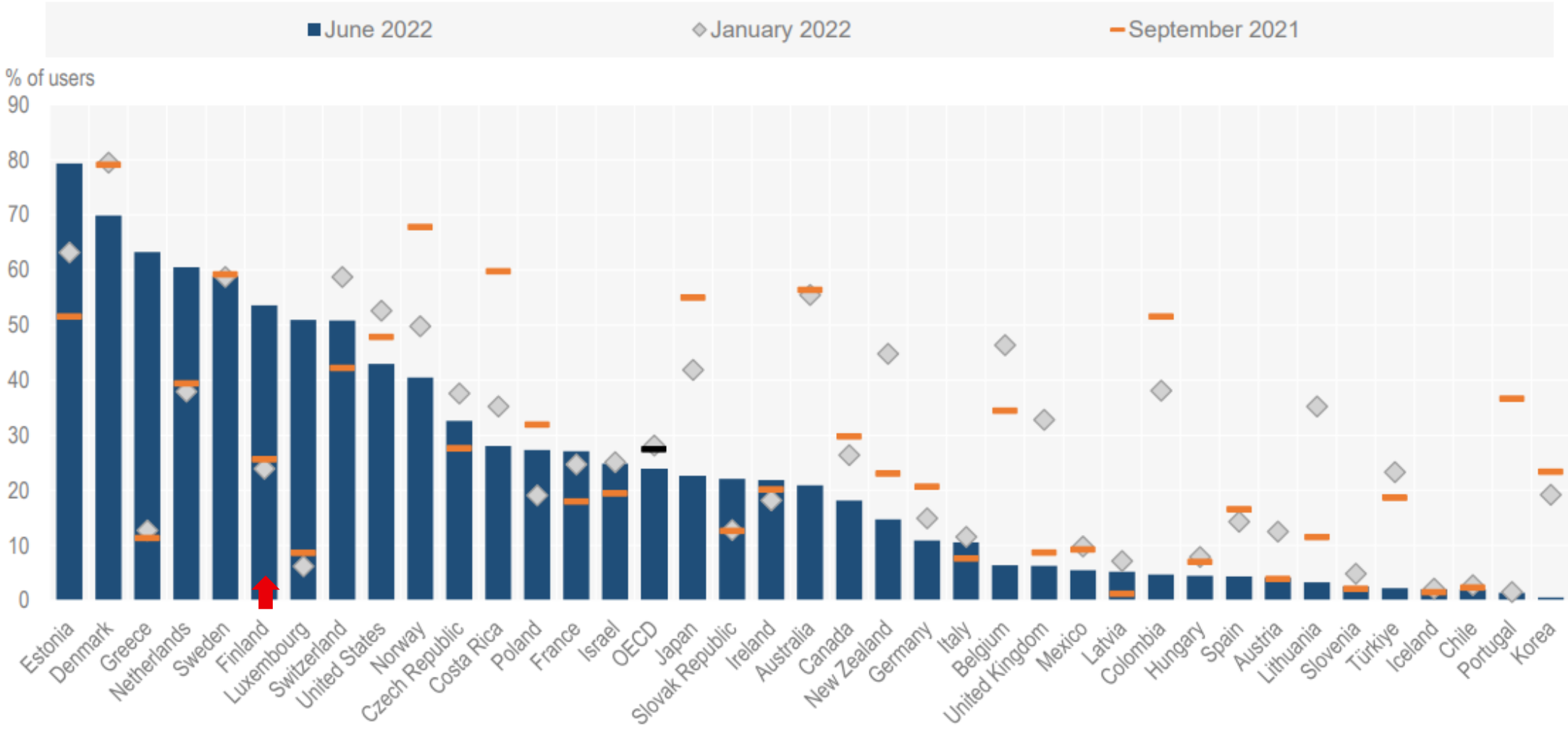


IPv6



… but ROAs provides no inherent benefit if ASes do not filter routes to drop RPKI invalid results.

Rate of ROV filtering in OECD countries (September 2021, January 2022, June 2022)



Source: OECD (2022), "Routing security: BGP incidents, mitigation techniques and policy actions", https://doi.org/10.1787/40be69c8-en.

Our planned actions to expedite the RPKI adoption

- We have planned 3-step approach to improve routing security among Finnish networks operators and owners:
  1. Promote general awareness of RPKI and speed up ROA signing especially among ISPs, Public sector and CIP
  2. Promote RPKI origin validation and invalid route dropping at least on IP transit operator and IXP level
  3. Promote new RPKI based technologies to be implemented when their maturity is at adequate level like BGPSec and ASPA
- We aim to be more *enabler* than authority, **how can we help?**
  - **Support** -> **Recommendation** -> **Regulation** (renewal of M67)

What to do next? aka homework!

- RPKI infrastructure is now in place and you should start using it!
- Publish those ROAs, its easy enough!
  - RIPE documentation and materials https://www.ripe.net/manage-ips-and-asns/resource-management/rpki/resource-certification-roa-management
- Prepare to implement RPKI based route origin validation to speed up future technologies adoption like BGPSec and ASPA
- If you need any assistance contact your local friendly regulator!

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Any questions?

Contact us:
cert@traficom.fi