Exploring Potential Use Cases for RPKI Signed Checklist (RSC) Under RFC 9323

An ARIN Community Grant Program

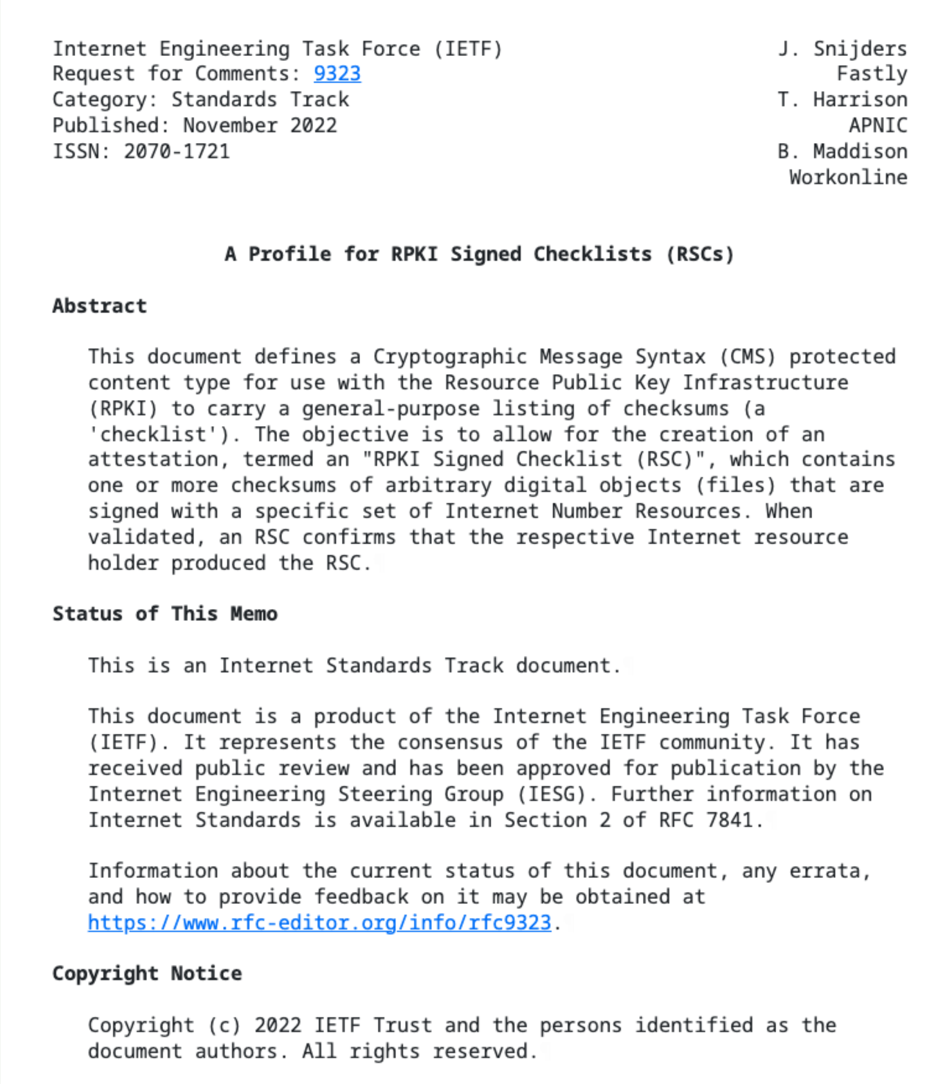
Internet Society

Dr. Amreesh Phokeer
Internet Measurement and Data Expert
phokeer@isoc.org

Background

- The Resource Public Key Infrastructure (RPKI) secures routing resources. The most common application of RPKI today is Route Origin Validation using the Route Origin Authorization (ROA) that asserts IP prefixes and the authorized origin ASN. Autonomous System Provider Authorization (ASPA) is another application of RPKI.

- RPKI Signed Checklists (RSCs) is a new type of RPKI object that came out in late 2022 (RFC9323). RSCs allow resource holders (prefix/ASN) to sign a list of hashing of arbitrary text with authorized resources they hold.



Internet Engineering Task Force (IETF)
Request for Comments: 9323
Category: Standards Track
Published: November 2022
ISSN: 2070-1721

J. Snijders
Fastly
T. Harrison
APNIC
B. Maddison
Workonline

A Profile for RPKI Signed Checklists (RSCs)

Abstract

This document defines a Cryptographic Message Syntax (CMS) protected content type for use with the Resource Public Key Infrastructure (RPKI) to carry a general-purpose listing of checksums (a 'checklist'). The objective is to allow for the creation of an attestation, termed an "RPKI Signed Checklist (RSC)", which contains one or more checksums of arbitrary digital objects (files) that are signed with a specific set of Internet Number Resources. When validated, an RSC confirms that the respective Internet resource holder produced the RSC.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9323.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

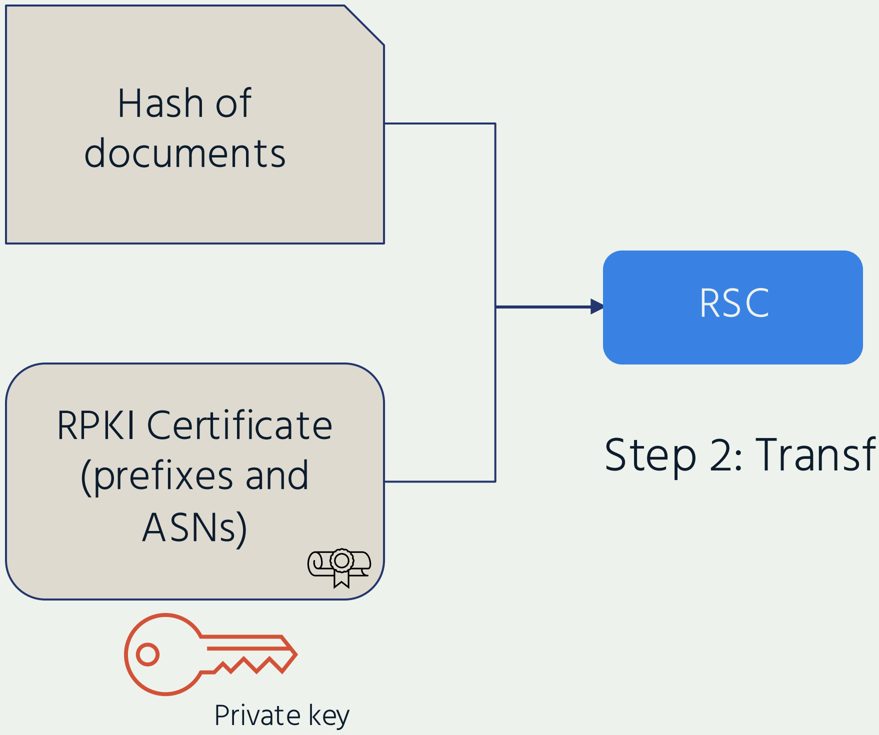
Motivation & Goals

What are the potential use cases of RPKI RSCs?

What is the current challenges of using RSCs and deploying software supports for RSCs?

Creation and verification of RPKI RSCs

Resource Holder



Hash of documents

RPKI Certificate (prefixes and ASNs)

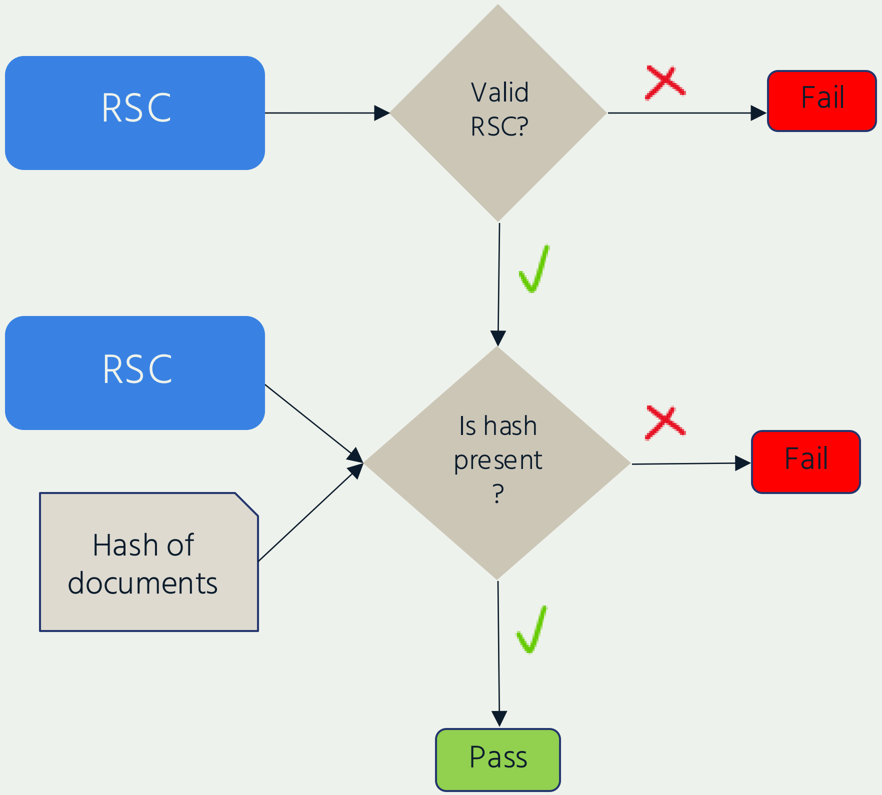
Private key

RSC

Step 2: Transfer OOB

Step 1: Creation

Third party



RSC

Valid RSC?

✗

Fail

✓

RSC

Hash of documents

Is hash present ?

✗

Fail

✓

Pass

Verification

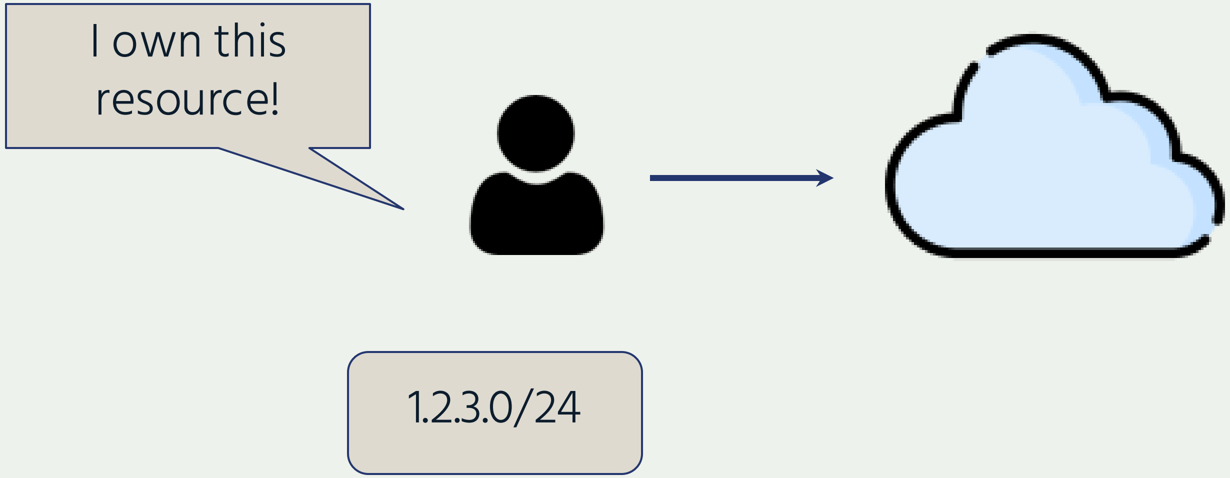
Potential Use cases of RPKI RSCs

Resource Ownership Verification

1. Bring Your Own IP Address (BYOIP)
2. Internet transit service
3. Routing information databases
4. Geolocation self-report

Bring Your Own IP Address (BYOIP)

- Customers could bring their own resources (prefix and ASN) to cloud providers
- Before onboard resources, the customer need to prove the ownership.



I own this resource!

1.2.3.0/24

Current Practice of BYOIP

WHOIS-based methods	• Email verification: Send verification link to the email address listed in WHOIS records • Random string: Put a random string in WHOIS record provided by the service providers • Self signed certificate: Put a self signed certificate in WHOIS record and provide public key
LOA (manual inspection)	Provide a LOA with the company name and resources
RPKI ROA	Add the cloud provider's ASNs to ROA
rDNS	Add a random record in rDNS provided by the cloud provider

Current Practice of BYOIP

Cloud Provider	WHOIS based method			ROA	LOA	rDNS
	Email Verification	Random String	Self signature			
Google Cloud				✓		✓
Amazon AWS			✓	✓		
Oracle Cloud			✓			
OVH Cloud		✓				
Vultr	✓			✓	✓	

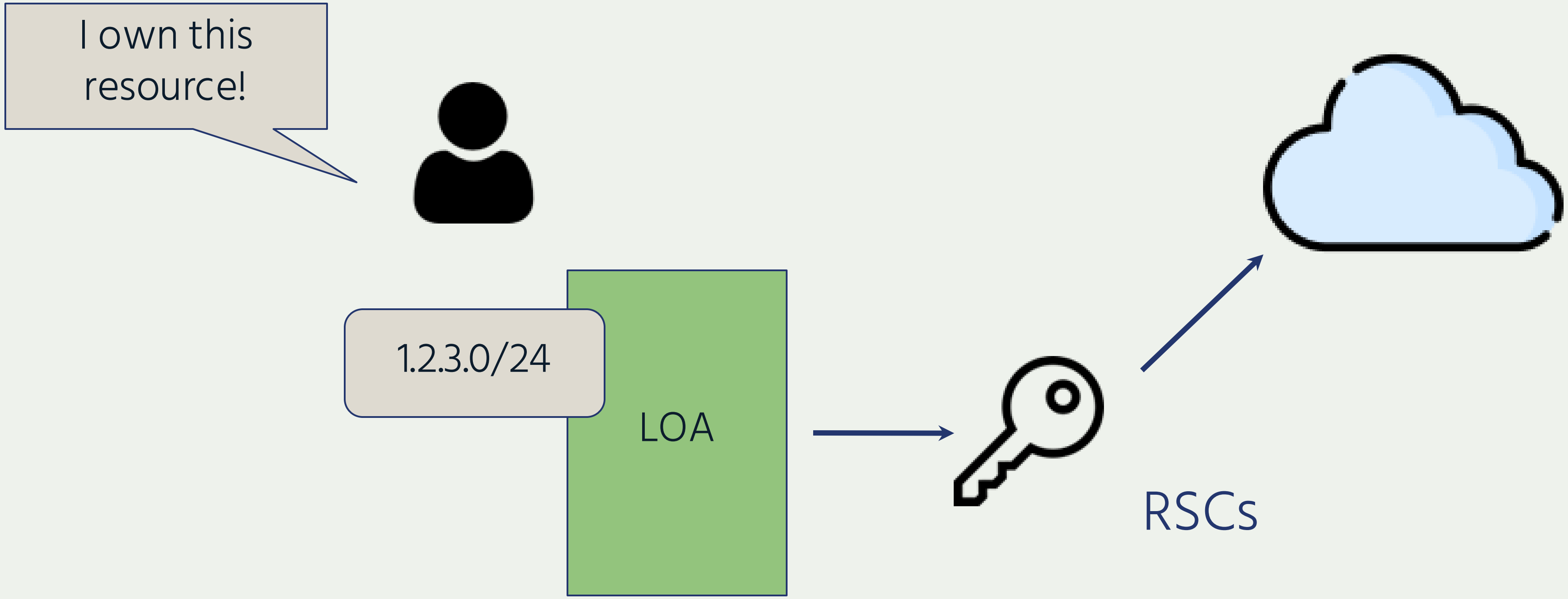
Challenges of Current Practice

Method	Security	Privacy	Easy to use
WHOIS: Email Verification	Subjected to Email security	✅	✅
WHOIS: Random String	✅	❌	❌
Whois: Self signature	✅	❌	❌
ROA	Can't use alone	✅	✅
LOA	LOA could be fake	✅	❌
rDNS	✅	❌	❌

Using RSCs for BYOIP

There are two ways to use RSCs for securing BYOIP:

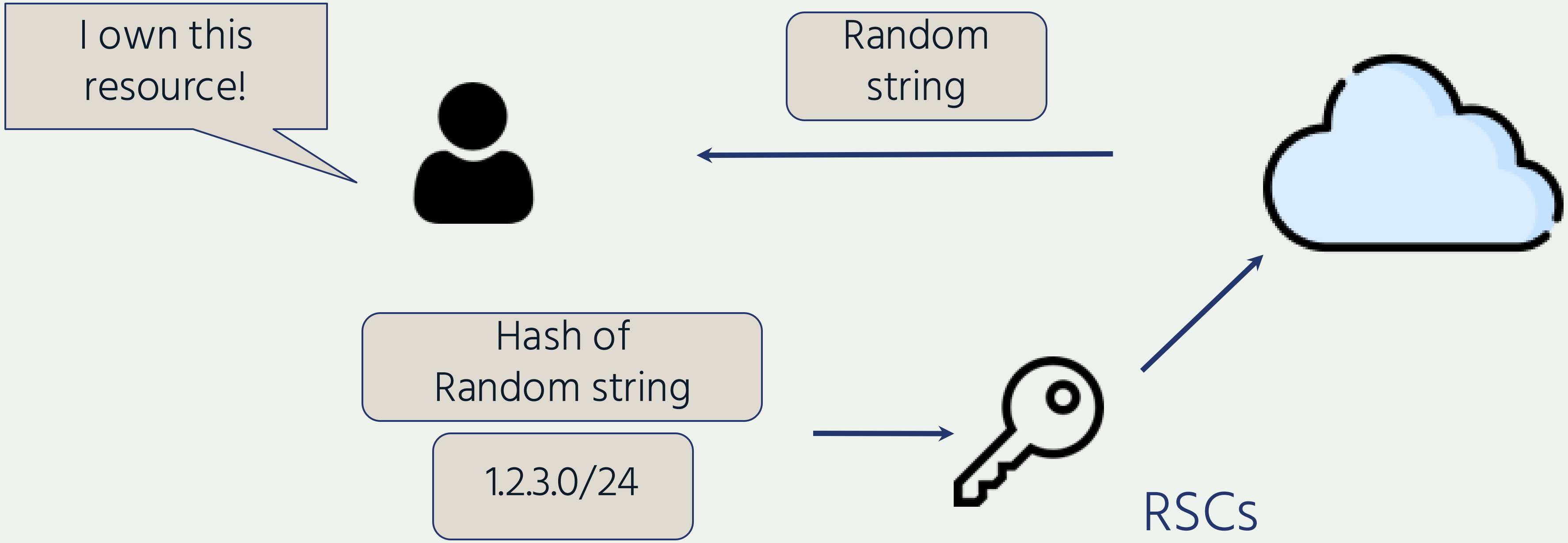
1. Use RSCs to sign the LOA



Using RSCs for BYOIP

There are two ways to use RSCs for securing BYOIP:

2. Signing random string

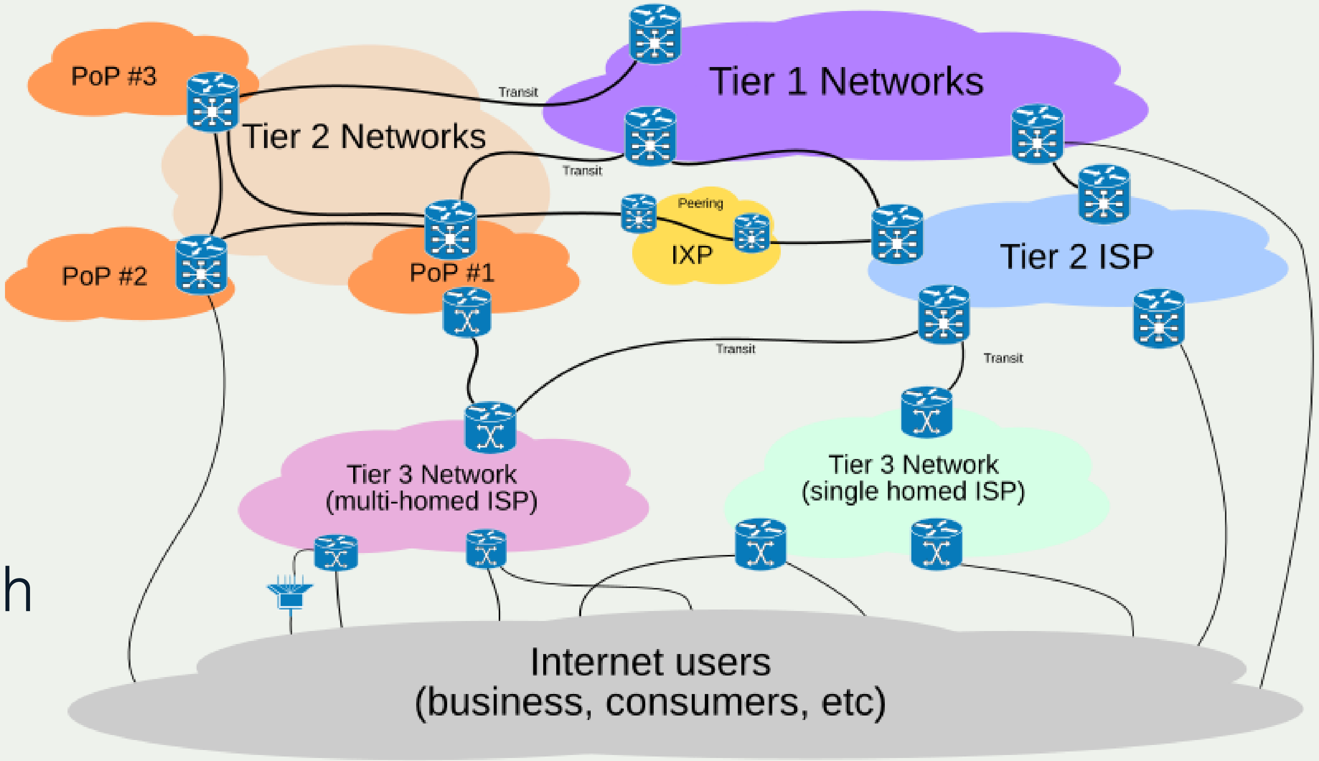


Use case: Internet Transit Service

Apart from Cloud providers, ISPs also require LOA to verify resource ownership during transit services.

How RSCs can be used:

Resource owners can sign the LOA with resources used for transit services.



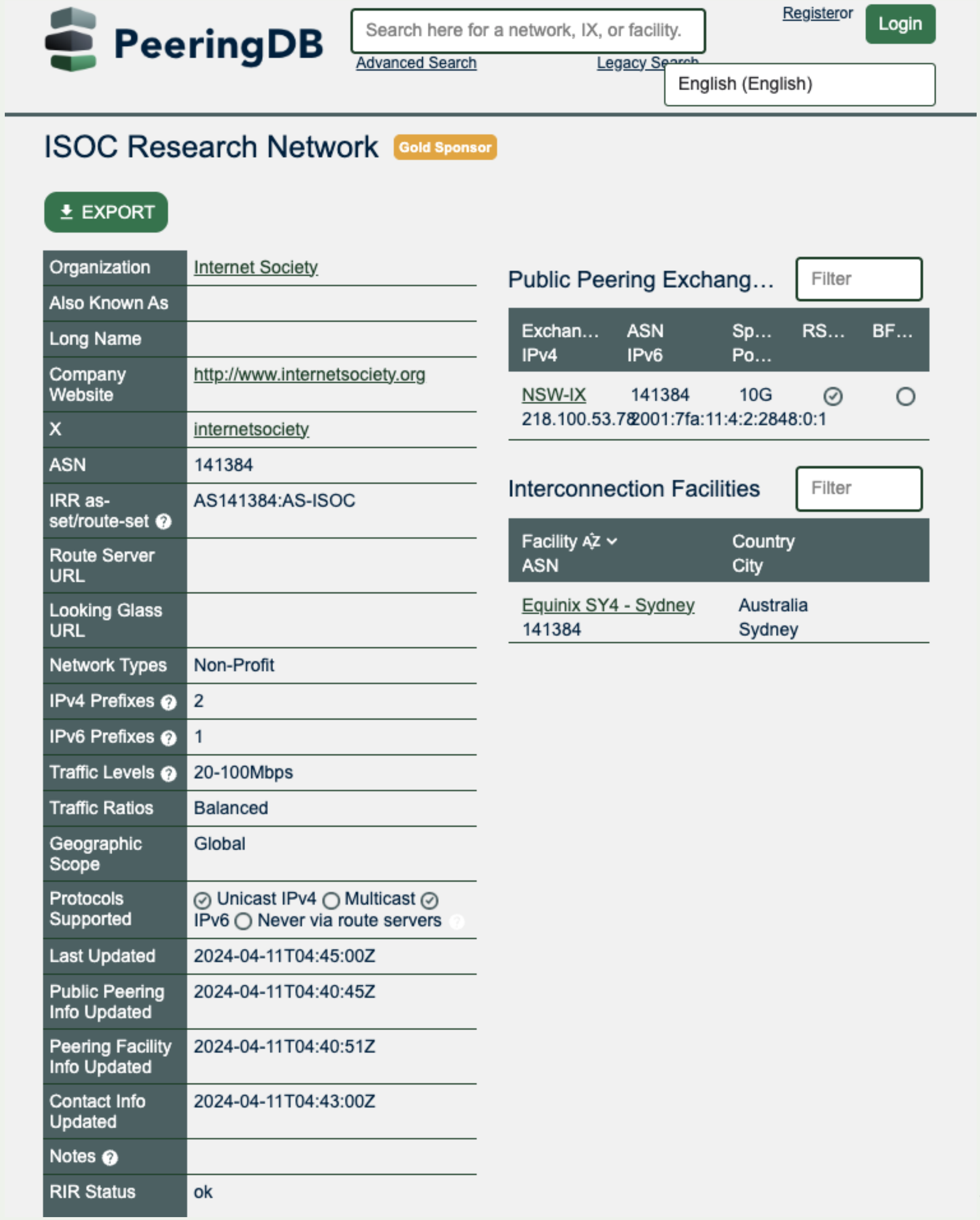
Representation of Internet Connectivity Distribution
Wikimedia Commons

Use case: Routing databases

Third party routing information databases like PeeringDB do not have the ground truth of resource ownerships. Currently PeeringDB relies on Whois record for ownership verification.

How RSCs can be used:

Resource owners can sign a specific content provided by PeeringDB with RSCs to claim the ownership of specific resources.



ISOC Research Network

Organization	Internet Society
Also Known As	
Long Name	
Company Website	http://www.internetsociety.org
X	internetsociety
ASN	141384
IRR as-set/route-set ?	AS141384:AS-ISOC
Route Server URL	
Looking Glass URL	
Network Types	Non-Profit
IPv4 Prefixes ?	2
IPv6 Prefixes ?	1
Traffic Levels ?	20-100Mbps
Traffic Ratios	Balanced
Geographic Scope	Global
Protocols Supported	✓ Unicast IPv4 ○ Multicast ✓ IPv6 ○ Never via route servers
Last Updated	2024-04-11T04:45:00Z
Public Peering Info Updated	2024-04-11T04:40:45Z
Peering Facility Info Updated	2024-04-11T04:40:51Z
Contact Info Updated	2024-04-11T04:43:00Z
Notes ?	
RIR Status	ok

Public Peering Exchang…

Exchan…	ASN	Sp…	RS…	BF…
IPv4	IPv6	Po…		
NSW-IX 218.100.53.78	141384 2001:7fa:11:4:2:2848:0:1	10G	✓	○

Interconnection Facilities

Facility A͢Z ⌄	Country
ASN	City
Equinix SY4 - Sydney 141384	Australia Sydney

Use case: Geolocation Report

Third party IP Geolocation databases like Google, IPinfo and maxmind allow resource owners to report their geolocations.

How RSCs can be used:

Resource owners can sign a specific content provided by Geolocation providers with RSCs to claim the ownership of specific resources.

How RSCs can be used

Current ownership verification methods, like WHOIS and LOA, are not suitable for continuous verification and revocation.

- Continuous verification: the verifier can continuously validate the RSCs during the service period.
- Revocation: resource owners can

Conclusion

RPKI RSCs can be widely used for Cloud services, Internet transit services, and variety of third-party databases.

Comparing with current ownership verification methods, RSCs have advantages on security (can't be fake) and privacy (won't be public, like WHOIS), provide continuous verifications,

Although current RSCs standard is already fully functional, it requires services providers to update their workflow to use it.

Survey - Results so far

- To gain insight into how network operators perceive RSC, identify potential use cases, and address real-world challenges.

- We conducted a survey during APRICOT 2025 in Malaysia (February 2025). We received over 35 responses,

- While that’s not a good representation of the entire region, it includes a diverse group of major operators such as Telstra, Telekom Malaysia, and Vocus, offering valuable industry perspectives.

Survey – Top barriers

- Lack of awareness/understanding (60%)
- Integration with existing RPKI infrastructure (40%)
- Unclear business benefits (30%)
- Regulatory/legal concerns (compliance, liability)

Interested in Testing/Reviewing

~50% of respondents are open to testing RSCs in a sandbox or pilot environment.

The other half are less certain and demand further evaluation before testing.

Survey Highlights

ROA vs. RSC

- Most respondents view RSC as complementary to ROA, especially for non-routing use cases.
- Some confusion about whether RSC is redundant or overlapping with existing ROA workflows.

Replacing LOAs

- ~40% believe RSCs could replace LOAs if formal attestations become the norm.
- ~30% object due to operational complexity or uncertainty.

Public vs. Private Repositories

- ~60% support public RSC repositories hosted by RIRs for transparency.
- Others prefer private repositories for internal use only, citing operational or security concerns.

Survey - Key Observations

RSC can apply to virtually any digital object.

Tools, documentation, and best practices must be clearer.

It can simplify or replace legacy LOA processes, if operational complexity is addressed.

We need more feedback from operators on real-world uses and best practices.

Survey - Help us understand better

This survey gathers insights on awareness, potential applications, challenges, and legal considerations related to RPKI Signed Checklists (RSCs) among network operators, enterprises, and cloud providers. Your responses will help shape best practices, inform discussions, and guide further standardisation efforts.

https://tinyurl.com/rpki-rsc-survey

Thank You

Dr. Amreesh Phokeer
Internet Measurement and Data Expert
phokeer@isoc.org