KISA 한국인터넷진흥원

KRNIC Update

Feb, 2026

Korea Network Information Center

Lee, Han Sang

KISA 한국인터넷진흥원

CONTENTS

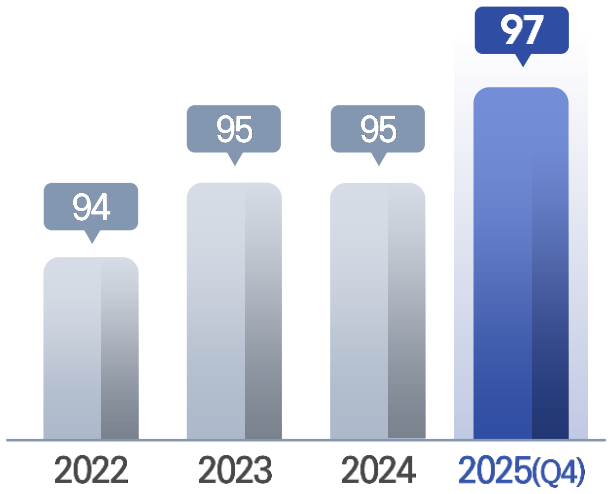
Internet Number Resources Statistics

I Statistics on KRNIC Members.

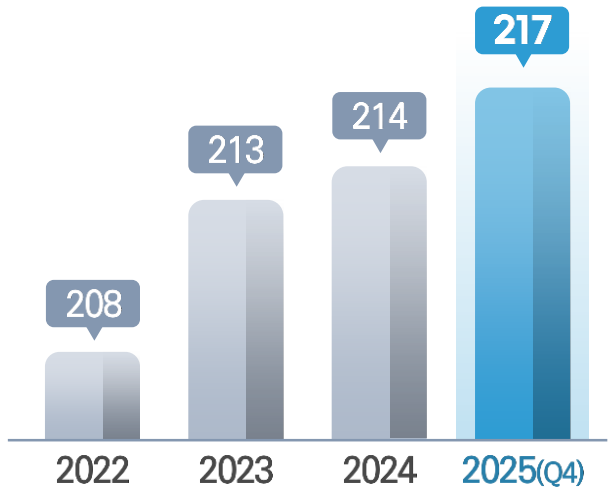
KISA 한국인터넷진흥원

Members

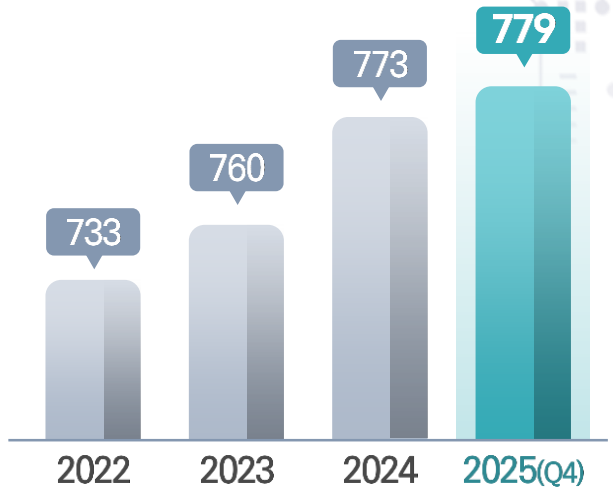
Internet Registries(ISP)



Direct Assignment Users

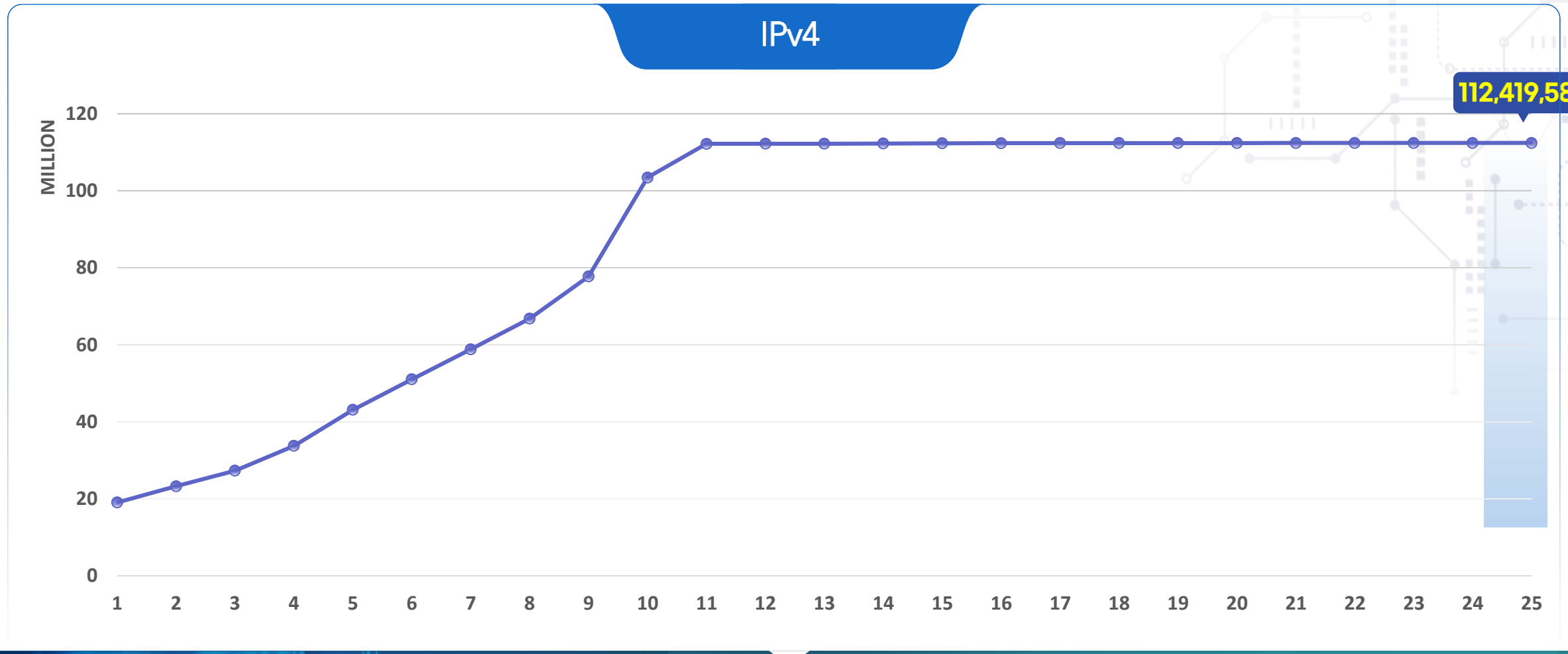


ASN Users



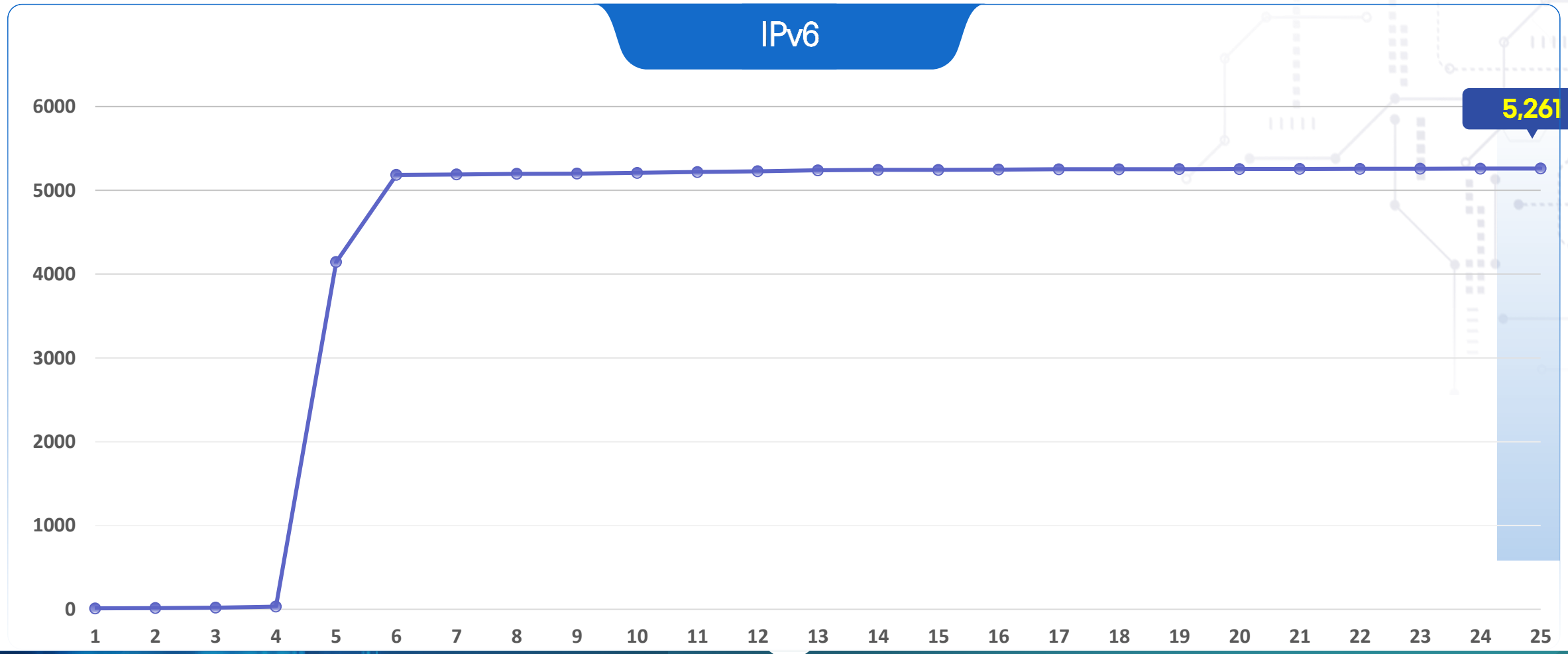
As of Q4 2025, KRNIC has a total 1,093 members.

I Statistics on IPv4 Allocations



As of Q4 2025, KRNIC has allocated 112,419,584 IPv4 addresses.

I Statistics on IPv6 Allocations



As of Q4 2025, KRNIC has allocated 5,261 IPv6 addresses. (/32)

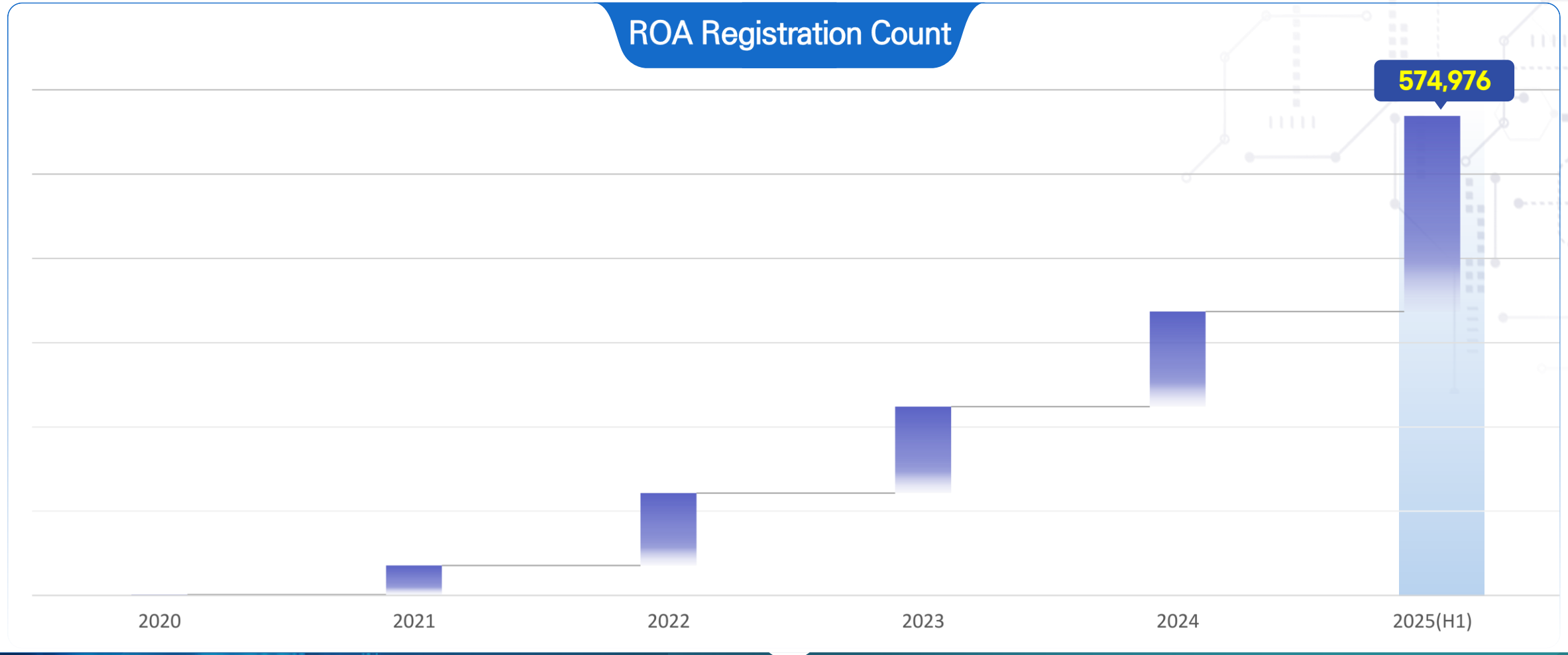
I Statistics on ASN Allocations

As of Q4 2025, KRNIC has allocated 1,105 ASNs. (2-byte: 895, 4-byte: 210)

II

KRNIC's RPKI Deployment Roadmap and Activity

I Number of ROA-Registered IPv4 in Korea



Korea's ROA-Registered Count is very low (2%)

Ⅱ KRINC's RPKI Deployment Roadmap

KISA 한국인터넷진흥원

	Step 1 (2026)	Step 2 (2027)	Step 3 (2028~)
	Preparation & Foundation	Pilot & Implementation	Expansion & Global Collaboration
RPKI Testbed System	Establishment & Preparation	Development & Pilot Operation	Expansion & Advancement
RPKI Deployment & Management	ISMP for RPKI System	Mgmt & Operation Pilot RPKI System	Wider Adoption for Service Providers
KRNOG Collaboration	Promotion with Large ISPs	Expansion to SMEs & Cooperation	Global Collaboration

Promote & Expand RPKI, Connecting NOGs

Ⅲ KRNIC's RPKI Routing Security Testbed

What is the RPKI Routing Security Testbed?

The RPKI Routing Security Testbed is a "virtual proving ground" where you can safely test routing security technologies before deploying them on the live Internet, preventing attackers from tampering with routing information like road signs on a highway.
It provides a controlled lab environment to emulate real-world Internet routing conditions and to validate that RPKI-based protection works as intended without impacting production traffic.

The RPKI Routing Security Testbed provides test equipment and full configuration support for routing security technologies like RPKI. It creates a structured environment to systematically validate RPKI deployment, performance evaluation, and incident response readiness.

01. Provision of a virtualized testbed infrastructure that reflects the global standard RPKI architecture

02. Simulation of realistic route hijacking attack scenarios to verify the effectiveness of RPKI deployment

03. Hands-on practice in building ROA registration and validation servers tailored to the domestic environment, enabling a safe transition to RPKI

04. Delivery of quantitative analysis reports based on empirical test data to support the definition of objective operational targets

05. Reservation and administrative support for the testbed, with priority given to organizations mandated to adopt RPKI

Purpose of the RPKI Routing Security Testbed

The testbed is designed to support reliable and secure adoption of RPKI through realistic mock deployments and systematic evaluation.
By enabling pre-deployment design, configuration, and assessment, it helps operators reduce the risk of misconfiguration, route hijacking, and other routing incidents when rolling out RPKI in production networks.

Securing stable RPKI deployment capabilities through pre-validation testing

Hands-on RPKI implementation practice in a virtual lab environment builds the technical expertise needed for reliable rollout.

Identifying RPKI deployment failure points and operational caveats

Through pre-production testbed simulations, operators can proactively detect and eliminate potential exception scenarios and latent failure factors before live deployment.

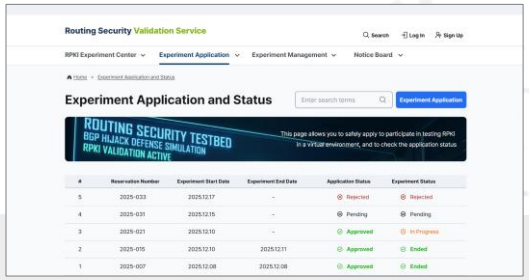
Support for establishing performance metrics and maintenance objectives

Leveraging performance and stability validation data from testbed experiments, operators can define optimized performance indicators and efficient maintenance targets tailored to their production environments.

Ⅲ KRNIC's RPKI Routing Security Testbed

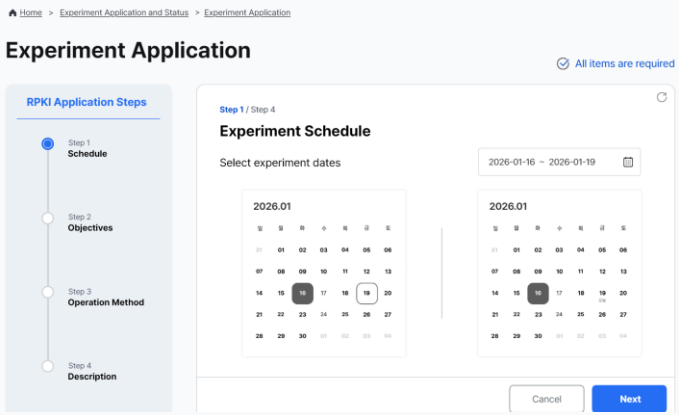
RPKI Routing Security Experiment Application Process

This portal enables organizations to request and track access to a secure virtual environment for safely testing RPKI, the critical technology that protects Internet routing paths from hijacking and manipulation.

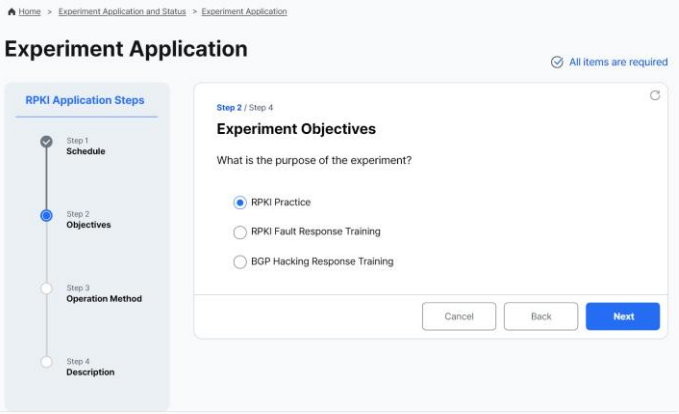


User Portal :
Experiment Application & Status Dashboard

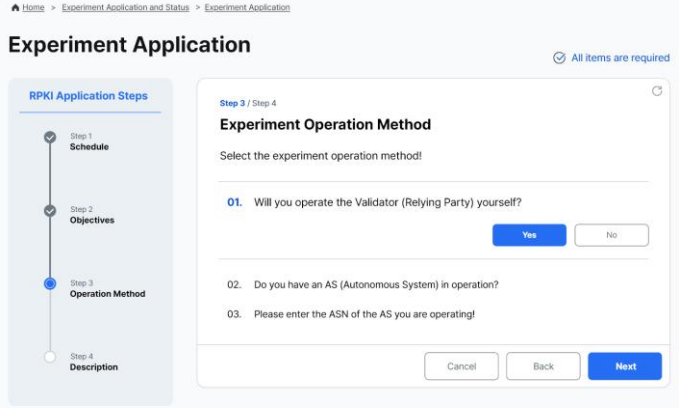
Experiment Application Workflow



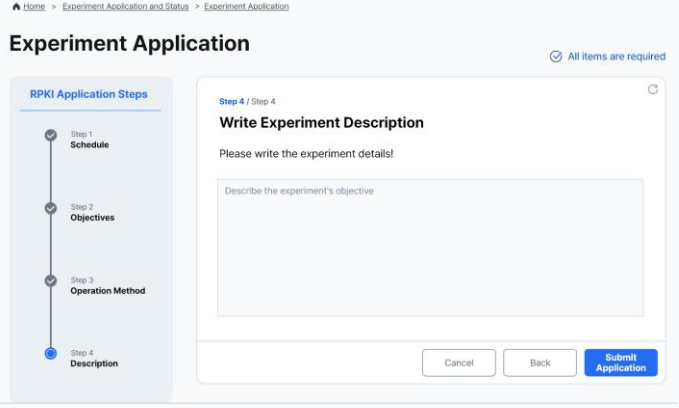
Step 1:
Select Experiment Schedule



Step 2:
Define Experiment Objectives



Step 3:
Review Experiment Operations



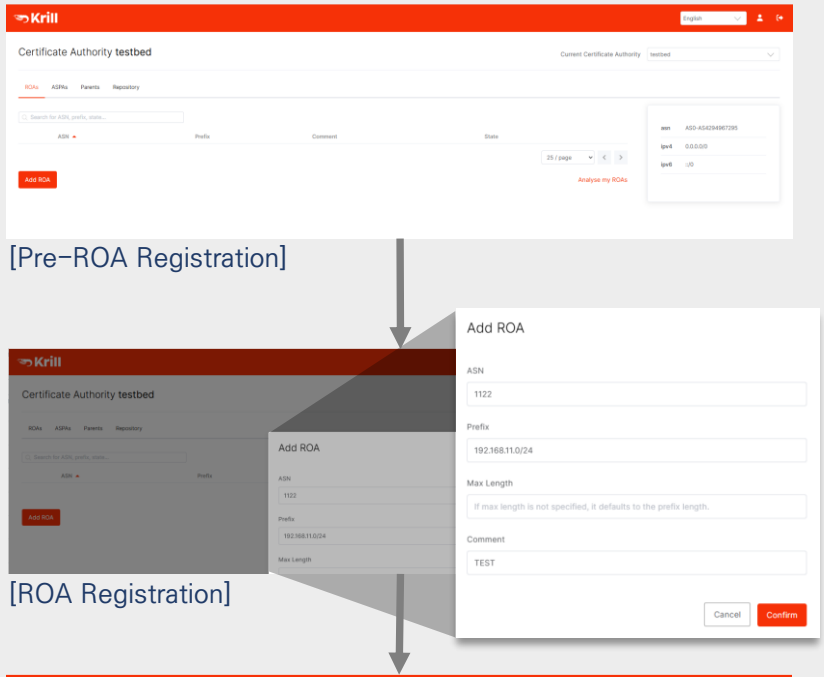
Step 4:
Submit Technical Experiment Description

Ⅲ KRNIC's RPKI Routing Security Testbed

ROA Issuance in Test Environment

Designates which networks are authorized to use specific IP address blocks, generating Route Origin Authorization(ROA) records to establish legitimate path ownership.

ROA Registration Workflow



[Pre-ROA Registration]

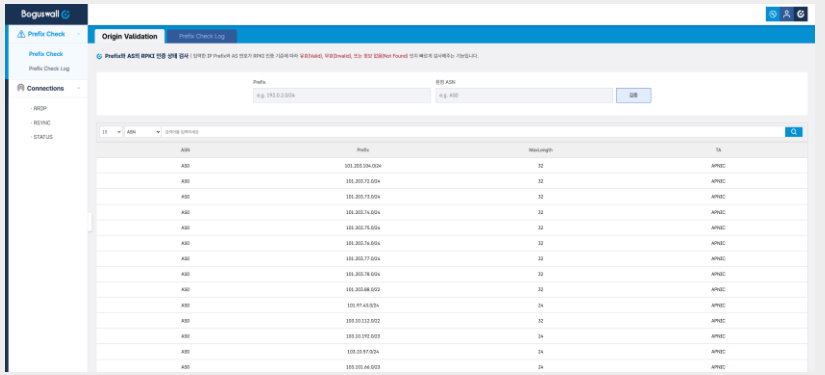
[ROA Registration]

[ROA Registration Complete]

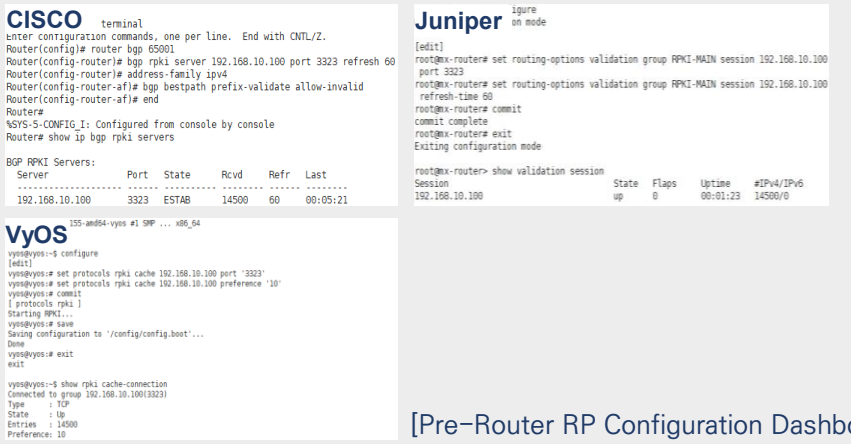
Test Environment Relying Party(RP) Deployment

Deploys Relying Party(RP) software to validate BGP route legitimacy, integrating with routers to activate the full RPKI security framework.

RP Deployment Screens(using Boguswall Commercial RP Solution)



[Relying Party(RP) Installation]



[Pre-Router RP Configuration Dashboard]

Ⅲ KRNIC's RPKI Routing Security Testbed

BGP Hijacking Response Experiment

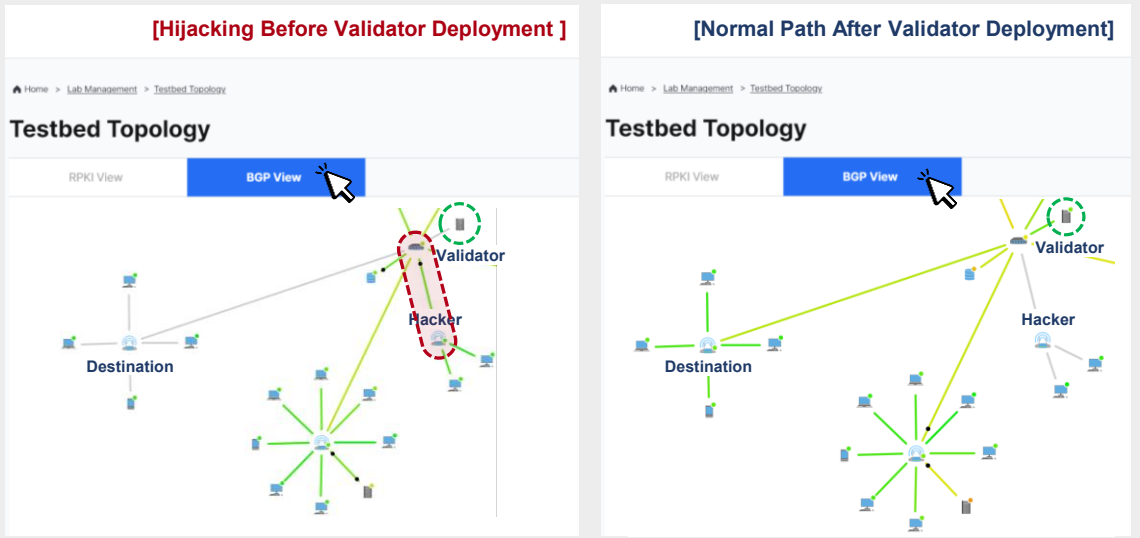
Interactive Visualization Dashboard

Designates which networks are authorized to use specific IP address blocks, generating Route Origin Authorization(ROA) records to establish legitimate path ownership.

Experiment Topology View(Testbed)

– BGP Perspective

BGP Hijacking scenario: Before & After RPKI deployment



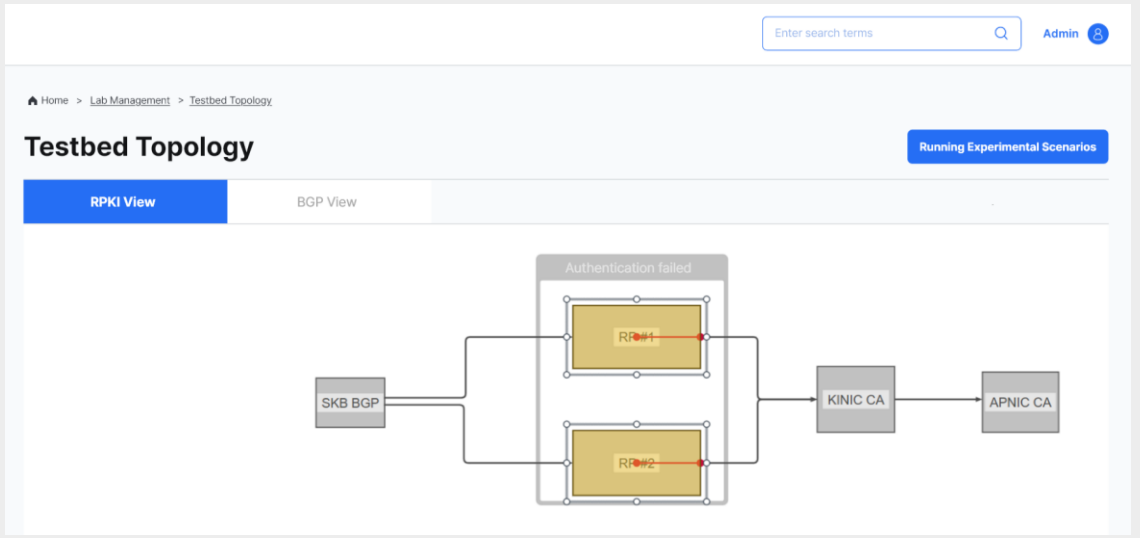
RPKI Routing Security Monitoring Practice

Real-time Validation Dashboard

Monitors whether your network (AS) is properly registered in RPKI and displays route validation status (Valid/Invalid/Unknown)

Experiment Topology View(Testbed)

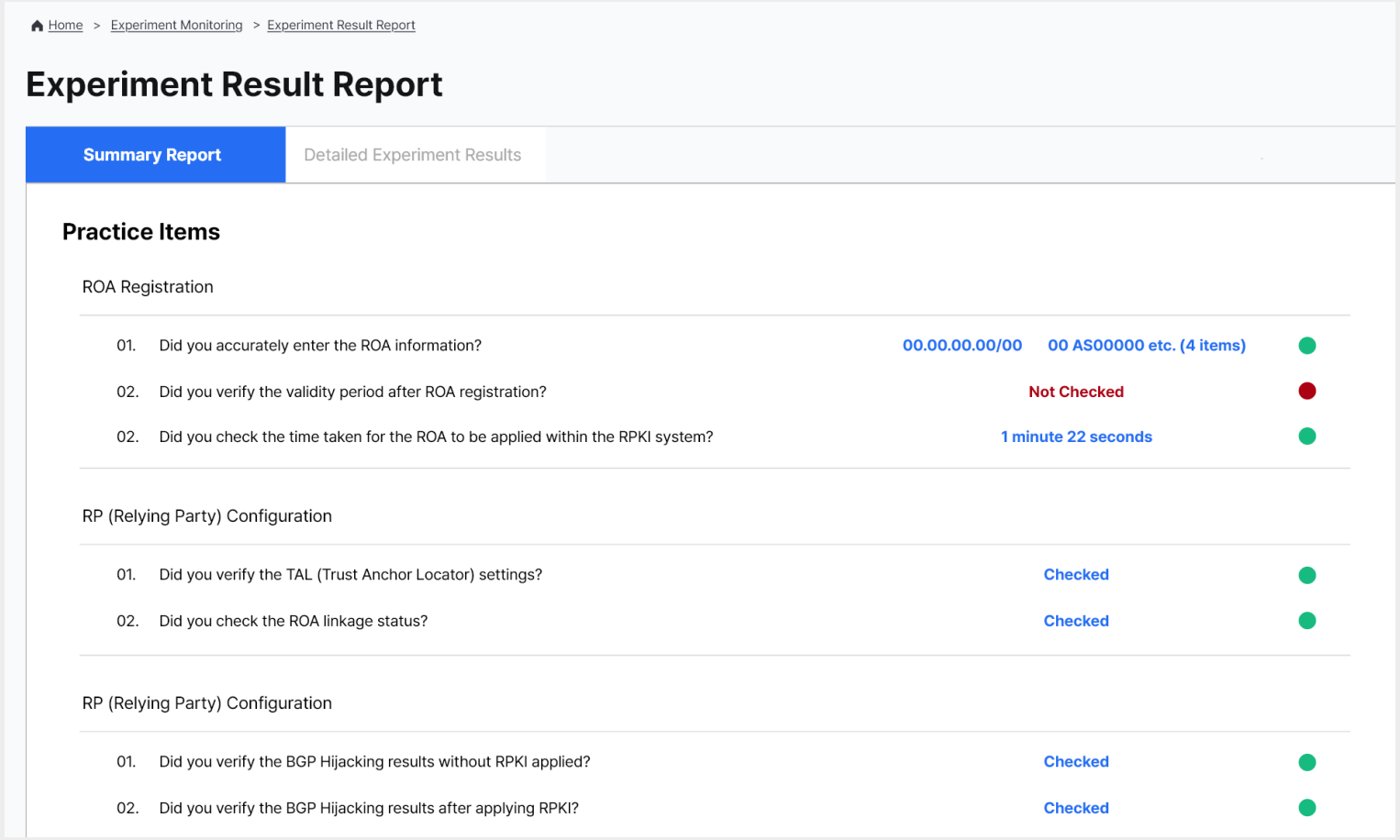
– RPKI Perspective



Ⅲ KRNIC's RPKI Routing Security Testbed

Results Report

Provides pass/fail reporting across 20 evaluation criteria covering key RPKI deployment procedures, enabling comprehensive learning and competency assessment of the RPKI implementation process



KISA 한국인터넷진흥원

Q&A