Operational and Deployment Considerations for Root KSK Algorithm Rollover

A Perspective from Emerging Internet Ecosystems

Nhat Huy Nguyen
Vietnam
Email: nguyennhathuybdi06@gmail.com

1 Introduction

This document provides technical and operational feedback on the proposed Root Zone KSK Algorithm Rollover. The transition from RSA/SHA-256 to ECDSA P-256 is a necessary step toward improving cryptographic efficiency and long-term sustainability of DNSSEC.

However, from the perspective of developing regions such as Vietnam, there remain practical challenges in deployment readiness, monitoring, and failure handling at the resolver and system level.

2 Key Observations

2.1 Gap in Resolver Readiness Visibility

While major DNS software supports ECDSA, there is limited visibility into:

- Real-world resolver compliance
- Misconfigured DNSSEC validation pipelines
- Legacy systems still dependent on RSA-only validation

This creates a risk where failures are only detected post-deployment.

2.2 Operational Risk in Double-Signing Phase

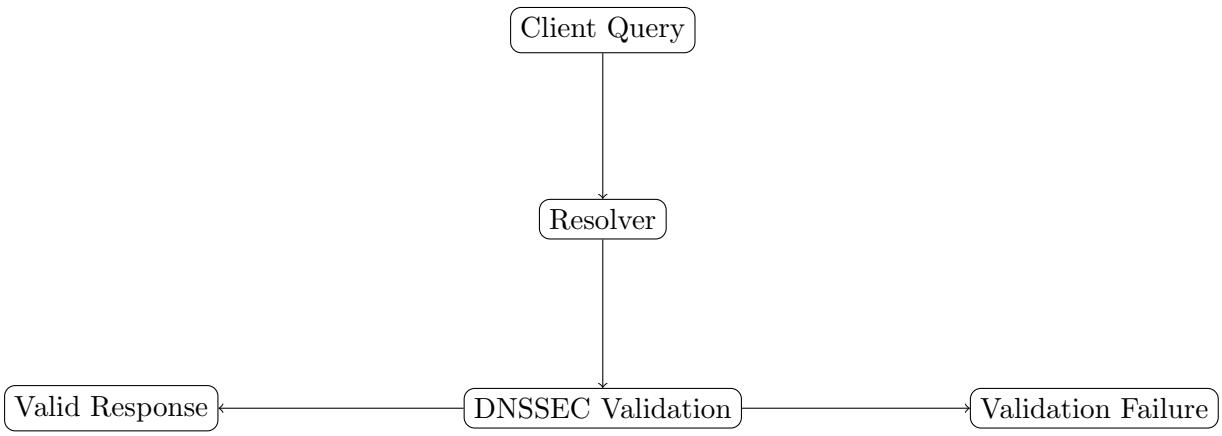
The double-signing phase increases DNS response size and complexity.

In environments with:

- Limited network reliability
- Improper MTU configuration
- UDP truncation issues

this may lead to increased fallback to TCP and degraded performance.

3 System-Level Risk Flow



This simplified model highlights the critical point where algorithm mismatch or incomplete trust anchor updates may lead to validation failure.

4 Recommendations

4.1 1. Monitoring and Telemetry

ICANN should encourage:

- Public dashboards tracking resolver readiness
- Metrics on DNSSEC validation failure rates
- Regional breakdown of adoption

4.2 2. Reference Testing Environments

Provide:

- Containerized DNSSEC testbeds
- Simulation tools for rollover scenarios
- Failure injection testing for resolvers

4.3 3. Operator-Focused Documentation

Current documentation is highly technical but lacks:

- Step-by-step deployment playbooks
- Troubleshooting scenarios
- Real-world failure case studies

4.4 4. Gradual Risk Mitigation Strategy

While the phased approach is strong, additional safeguards could include:

- Extended observation periods between phases
- Public reporting checkpoints before phase transitions

5 Conclusion

The proposed Root KSK algorithm rollover is well-structured and technically sound. However, successful global deployment depends not only on cryptographic design, but also on operational readiness across diverse environments.

Bridging the gap between specification and real-world deployment—especially in developing regions—should be a priority to ensure a smooth and secure transition.