



# Problem Statement 03

## Post-Quantum DNSSEC Testbed under a Delegated .IN Domain

[Reference: PQIP WG & PQDNSSEC Side meetings](#)

### Background

With the advent of quantum computing, the cryptographic foundations of DNSSEC (RSA, ECDSA) are at risk. The Internet community is actively researching Post-Quantum Cryptography (PQC) for DNSSEC, ensuring trust anchors and zone signatures remain secure in a quantum era. Instead of experimenting at the .IN TLD level, this challenge leverages a delegated Second-Level Domain (SLD) under .IN (research-only, non-production) as a controlled testbed.

### Challenge

Design, deploy, and benchmark a **PQC-enabled DNSSEC testbed** on a delegated .IN subdomain. The testbed will host PQC-signed zones, validate resolution behavior, and provide operational insights for future adoption.

### Core Tasks

1. Delegated PQC Testbed Setup
  - Establish a delegated SLD (e.g., pqc-research.in) for hosting PQC-signed zones.
  - Ensure delegation is properly anchored and resolvable by test resolvers.
2. Prototype Authoritative Servers
  - Implement **PQC-compliant authoritative DNS servers** for the delegated SLD.
  - Track resolver fallback behavior over UDP/TCP due to large PQC signatures.
3. Performance & Abuse Scenario Analysis
  - Study **performance bottlenecks** (e.g., packet fragmentation, increased latency, CPU cost).
  - Simulate **TTL abuse scenarios** and evaluate caching impacts under PQC.
4. Benchmarking with AIORI Nodes
  - Use **AIORI Internet Measurement Nodes (IMNs)** distributed across India for benchmarking.
  - Compare multiple PQC algorithms (e.g., Dilithium, Falcon, SPHINCS+) for latency, memory, and bandwidth trade-offs.
5. Protocol Validation & Standards Feedback
  - Validate compatibility with **PQDNSSEC proposals** (IETF discussions).
  - Document operational insights and prepare feedback for PQDNSSEC Working Group.



## Deliverables

- A working **delegated .IN SLD PQC-signed zone** with resolver validation demo.
- **Performance benchmarking report** (latency, packet size overhead, resolver fallback).
- Comparative results across **candidate PQC algorithms**.
- A concise **IETF feedback note** summarizing testbed learnings for PQDNSSEC.