# From Standard to Reality: DNS Security in .TH Operations

Titipong Pakinsri <titipong@thains.co.th>

May 26, 2026

THAINOG Day 2026

Thai Network Operators Group

# .th ccTLD Overview of DNS Infrastructure

| .th — Country-code Top-Level Domain | | |
|---|---|---|
| TLD Manager | THNIC Foundation | Policy-driven |
| Operator | Thai Name Server Co.,Ltd. | Back-end Registry Operator |
| Name Servers | 6 Name Server / 6 AS prefixs<br>Anycast-capable | High redundancy<br>DDoS mitigation |
| DNSSEC | Full DNSSEC Signing<br>DS in Root | Chain of trust verified globally |
| Connectivity | Dual-stack IPv4/IPv6<br>Multi-datacenter | Future-proof connectivity |

*https://www.iana.org/domains/root/db/th.html*

# Thai Name Server: TLD Consulting Service

## WHY YOUR OWN TLD?

**SHARED NAMESPACE**
`yourbank.com`
Brand lives below the dot

**YOUR BRAND IS THE TLD**
`intranet.yourbank`
Full ownership above the dot

## WHO IS THIS FOR?

| Finance | Government | Corporate |
|---|---|---|
| `.yourbank` | `.moph .moe` | `.brand` |

## OUR ROLE — REGISTRY CONSULTANT

| | |
|---|---|
| **Application** | Prepare & submit New gTLD application to ICANN |
| **Technical** | Registry system · EPP · DNSSEC · Zone signing |
| **Monitoring** | 24/7 uptime, latency & query performance — Nagios & Zabbix |
| **Security Mon.** | Real-time anomaly detection — DDoS, NXDOMAIN flood, traffic spike alerting |
| **Operations** | Ongoing DNS infrastructure & compliance management |

*"Stop renting a namespace — **own the top of your internet.**"*

# Best Practices in Action: Securing the .th

**1. Infrastructure Resilience & Diversity for .th DNS**

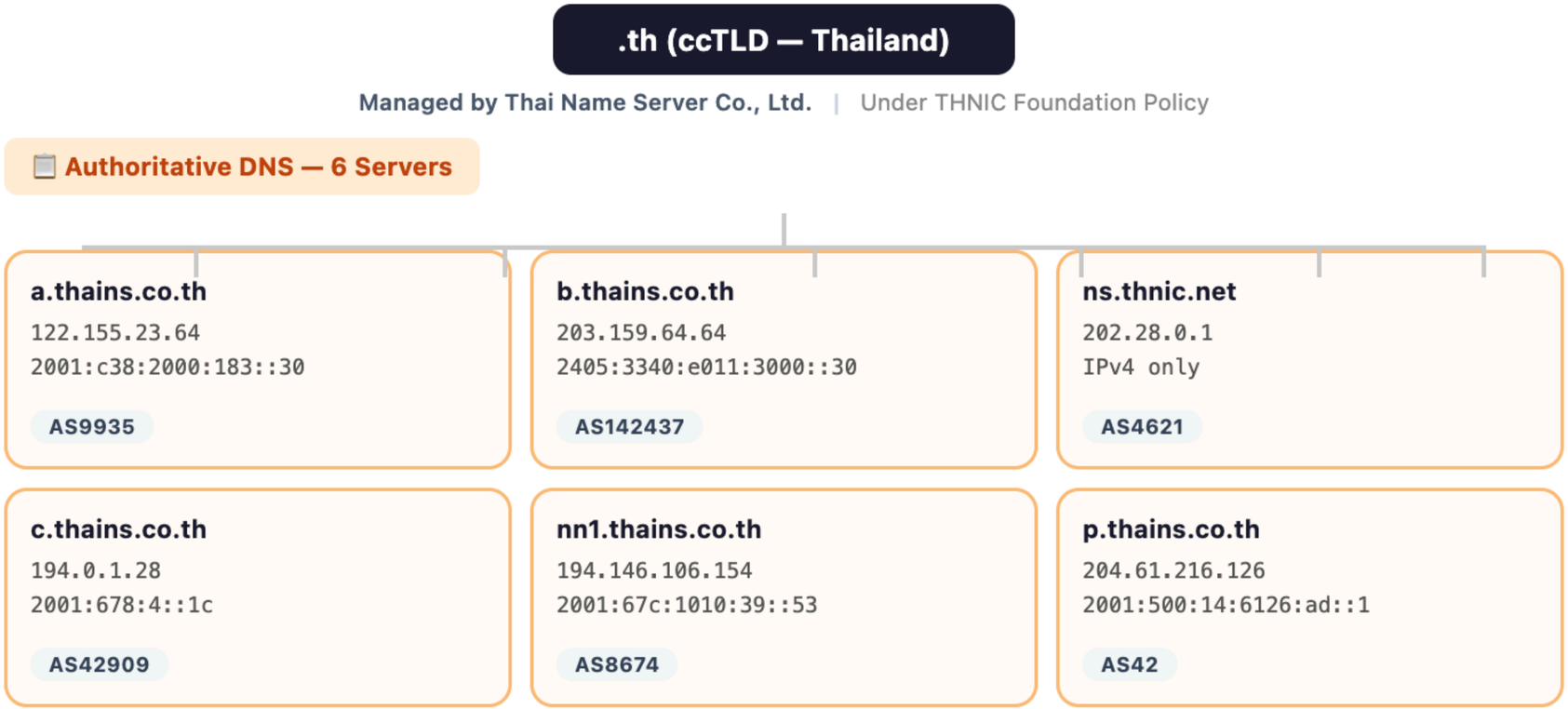
- .th DNS Diversified Infrastructure
  - Multi-Region - 3 Unicast and 3 Anycast Network
  - Multi-Vendor - 3 On-Premise and 3 Vendor
  - Multi-ASN - AS9935, AS142437, AS42909, AS42, AS8674, AS4621
- .th DNS Separate Infrastructure
  - Authoritative
    - a.thains.co.th, b.thains.co.th, c.thains.co.th
    - nn1.thains.co.th, p.thains.co.th, ns.thnic.net
  - Recursive
    - double7.thains.co.th

# Best Practices in Action: Securing the .th

**1. Infrastructure Resilience & Diversity for DNS .th**

- Minimum 2 Nameservers
  - The .th Reality: We go beyond the minimum. The .th zone is supported by six authoritative nameservers.
- Software Diversity
  - 3 On-Premise Nodes running BIND.
  - 3 Vendor Nodes running other software.

# Best Practices in Action: Securing the .th



# Best Practices in Action: Securing the .th


✓ **Separate Infrastructure:** Authoritative and Recursive run on different IPs and different roles

✓ **Reduced Attack Surface:** DDoS against Recursive (203.159.77.77) does not directly impact Authoritative servers

✓ **Separate ASN:** Recursive (AS141362) is on a different ASN from all Authoritative servers — good network-level separation

# Best Practices in Action: Securing the .th

**2. Security & Data Integrity**

- DNSSEC Signing for .th: The Chain of Trust
  - Algorithm 8 (RSA-SHA256): Balance of broad compatibility and robust.
  - Next Step: Transition to Algorithm 13 (ECDSA P-256) or above.
  - NSEC3 Support: Implementing Opt-out for zone walking protection.
- Zone File Integrity:
  - Automated pre-deployment validation for 100% accuracy.
  - Access Control, Authorized personnel only, restricted to trusted networks.
  - Audit Logging, Full traceability of all system and data modifications.
- Access controls on DNS server
  - Key-based Authentication: use of SSH Keys with strong passphrases
  - Network Access Control: Strict IP Whitelisting to restrict SSH access only
  - VPN Encapsulation: All management traffic is encapsulated.

# Best Practices in Action: Securing the .th

### 3. Key & Zone Lifecycle Management

- Key Management for .th:
  - Secure Key Storage: Strict access control for KSK/ZSK handling.
  - Key Rollover Policy: Scheduled and safe key rotations to ensure continuity.

- SecueZone Transfers
  - TSIG-Signed Transfers: Authentication for all data exchanges between nodes.
  - Access White-listing: Restricting zone transfers to authorized servers only.

# Best Practices in Action: Securing the .th

ZONE TRANSFER SECURITY · LIVE TEST

**dig @a.thains.co.th th. AXFR**

Zone Transfer Blocked

bash — 80×24

```
# Test 1: AXFR without TSIG
titipong@macbook ~ % dig @a.thains.co.th th. AXFR
; Transfer failed.
;; ->>HEADER<<- status: REFUSED, QUERY: 1, ANSWER: 0, AUTHORITY: 0

# Test 2: AXFR with wrong TSIG key
titipong@macbook ~ % dig @a.thains.co.th th. AXFR -y hmac-sha256:test:dGVzdA==
; Transfer failed.
;; ->>HEADER<<- status: NOTAUTH, TSIG error: BADSIG, ANSWER: 0

# Test 3: Normal SOA query
titipong@macbook ~ % dig @a.thains.co.th th. SOA
;; ->>HEADER<<- status: NOERROR, QUERY: 1, ANSWER: 1
th. 1800 IN SOA a.thains.co.th. registry.thains.co.th. 1260525082

✓ SOA query → NOERROR (normal queries answered)
✗ AXFR no TSIG → REFUSED (0 records transferred)
✗ AXFR wrong TSIG → NOTAUTH (BADSIG — key rejected)
```

# Best Practices in Action: Securing the .th

**4. Operational Monitoring & Visibility**

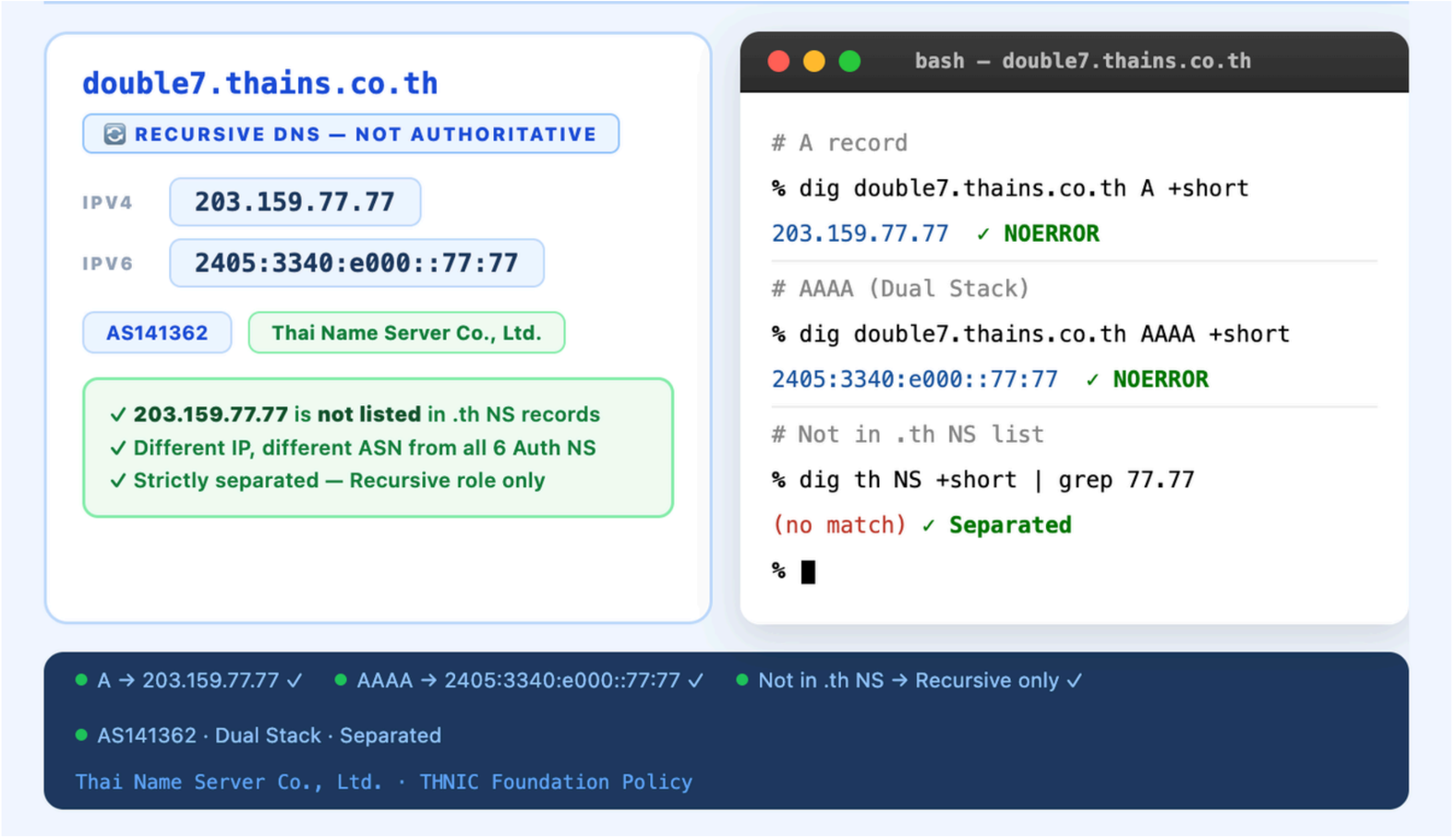
- DNS Monitoring:
  - 24/7 Real-time Monitoring
  - Tracking latency and availability across all nodes.
- Alerting & Logging:
  - Automated notifications for DNSSEC expiration
  - Automated alerts for abnormal QPS (Queries Per Second) spikes.

# Best Practices in Action: double7.thains.co.th

**1. Infrastructure & Software Diversity**

- Diversified Anycast Load Distribution:
  - Leveraging BKNIX to keep DNS traffic local.
  - Infrastructure is distributed across 3 distinct Data Centers
  - At least 2 VMs per site
- Infrastructure Isolation:
  - Complete physical and logical separation from Authoritative systems.
- Software Diversity
  - Running a hybrid BIND and Unbound stack on all nodes.

# Best Practices in Action: double7.thains.co.th



# Best Practices in Action: double7.thains.co.th

**2.Security & Validation**

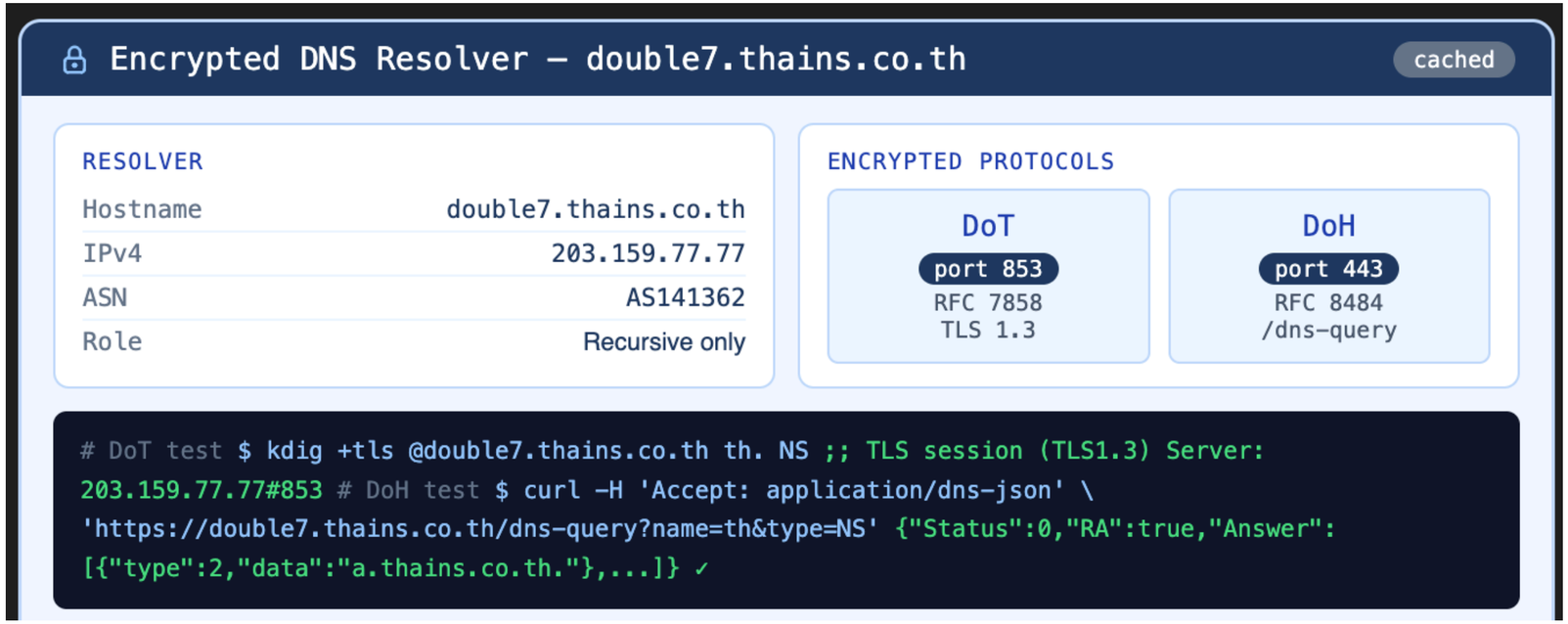
- DNSSEC Validation Enabled:
  - Prevents DNS Cache Poisoning
  - Invalid DNSSEC signatures are rejected immediately with SERVFAIL
- Response Rate Limiting (RRL):
  - Prevents DNS amplification/reflection attacks
- Access controls on DNS server
  - Key-based Authentication: use of SSH Keys with strong passphrases
  - Network Access Control: Strict IP Whitelisting to restrict SSH access only
  - VPN Encapsulation: All management traffic is encapsulated.
- Version Control
  - Git-Based

# Best Practices in Action: double7.thains.co.th

**3.Privacy & Modern Standards**

- QNAME Minimisation
  - double7.thains.co.th transmits only the minimum necessary information to each upstream server — never the full query name.
- Encrypted DNS
  - DNS over TLS (DoT) Enabled
  - DNS over HTTPS (DoH) Enabled

# Best Practices in Action: double7.thains.co.th



# Best Practices in Action: double7.thains.co.th

**4. Monitoring & Performance**

- 24/7 Operational Visibility
  - Any service degradation triggers immediate alerting to the NOC team.
- Service & Availability Monitoring:
  - Uptime, DNS port 53/853/443, DNSSEC validation state
  - alert on-call
- Performance & Capacity Monitoring:
  - Query rate (QPS), Response latency, CPU/RAM/disk, network throughput
- Real-time Anomaly Detection
  - Alerts on service failure
  - detects performance anomalies
  - Threats are identified and escalated before end users are impacted

# KINDNS Self-Assessment - .th ccTLD Scorecard

| Authoritative DNS Operator | | Core Hardening | | Registry / Registrar | |
|---|---|---|---|---|---|
| DNSSEC Deployment | ✅ Implemented | ACL Network Control | ✅ Implemented | Registry Lock | ✅ Implemented |
| Zone Transfer Restriction | ✅ Implemented | Config Access Control | ✅ Implemented | EPP Security | ✅ Implemented |
| Multiple NS ≥ 2 | ✅ Implemented | BCP38/MANRS | ✅ Implemented | HTTPS + TLS | ✅ Implemented |
| Infra Diversity | ✅ Implemented | Version Control | ✅ Implemented | Registrant 2FA | ✅ Implemented |
| Auth/Rec Separation | ✅ Implemented | MFA Console | ✅ Implemented | Credential Hygiene | ✅ Implemented |
| DNS Monitoring | ✅ Implemented | 2FA Customer | ✅ Implemented | — | — |
| Software Diversity | ✅ Implemented | — | — | — | — |

# Securing the .th Ecosystem: Enable DNSSEC Today

We invite all 3rd-level domain holders (e.g., .co.th, .in.th, .ac.th) to enable DNSSEC and strengthen our digital landscape:

- **Complete the Chain of Trust:** Establish a seamless cryptographic path from the .th Root to your domain, ensuring 100% data authenticity.
- **Prevent DNS Hijacking:** Protect your users from cache poisoning and fraudulent redirects using secure digital signatures.
- **National Cyber Resilience:** Contribute to a safer Thai internet by building a trusted environment for all digital transactions.
- **Ready for Implementation:** Our Registry infrastructure is fully prepared to accept your DS (Delegation Signer) records immediately.

*“Completing the Chain of Trust for 3rd-Level Domains”*

*www.checkdnssec.in.th*

# Q & A

**Titipong Pakinsri**
**titipong@thains.co.th**