DNS & DNSSEC operational best practices

Sleep better at night with KINDNS in your network!

These materials are licensed under the Creative Commons Attribution 4.0 International licence.
http://creativecommons.org/licenses/by/4.0/

Acknowledgements

- NSRC funds my time and my travel
- KINDNS is an ICANN initiative

KINDNS: background

KINDNS /ˈkaɪndnəs/ (noun) **K**nowledge-Sharing and **I**nstantiating **N**orms for **D**NS and **N**aming **S**ecurity

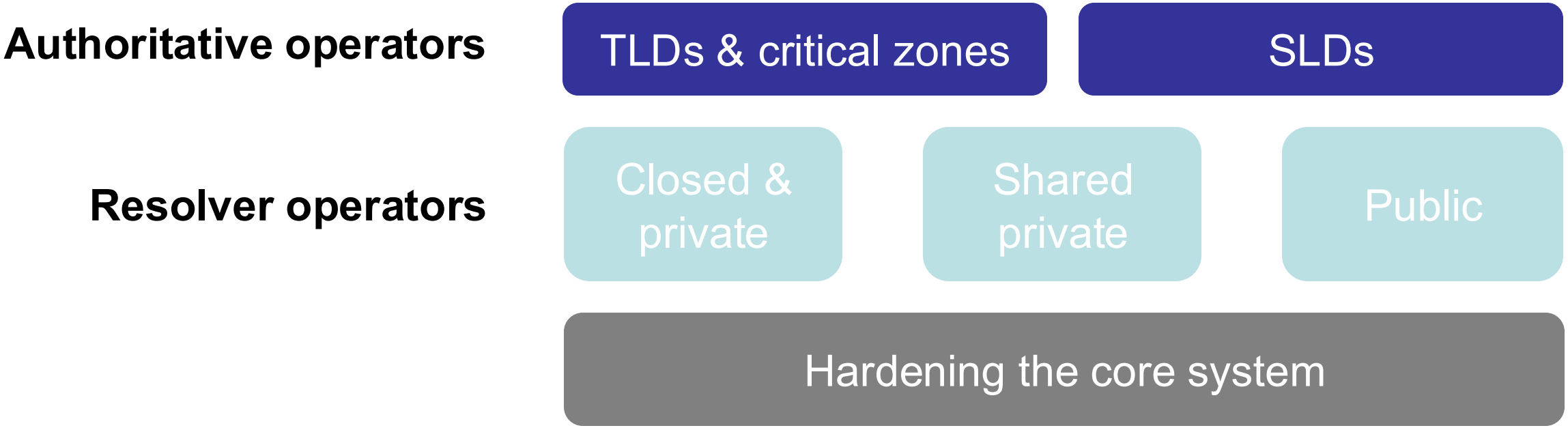
A simple framework that can help a wide variety of DNS operators, from small to large, to follow both the evolution of the DNS protocol and the best practices that the industry identifies for better security and more effective DNS operations.

See also: https://kindns.org

What kind of DNS operator are you?

- KINDNS “core guidelines” for everyone
- Additional guidelines for different deployments:
  - TLDs and critical zones
  - Public recursive resolvers
  - Other second-level domains
  - Shared recursive resolvers
  - Private infrastructure not reachable from the open internet
- No “One Size Fits All” checklists!

KINDNS: targeted operators



By joining the KINDNS initiative, DNS operators are voluntarily committing to adhere to the identified practices and act as “goodwill ambassadors” within the community.

Basic common-sense guidelines for DNS operations of all shapes and sizes

CORE GUIDELINES (FOR EVERYONE)

Core guidelines (for everyone)

1. ACLs restrict traffic to DNS servers
2. BCP38 egress filtering
3. DNS servers run DNS and nothing else
4. Access to DNS servers by DNS operators only
5. DNS configuration in revision control
6. Restrict access to management interfaces
7. Management access control with cryptographic keys or 2FA
8. User access control following sound credential management

ACLs restrict traffic to DNS servers

- Only permit DNS traffic inbound
  - TCP & UDP 53
  - If DoT also 853
  - If HTTPS also 443
- Only permit necessary outbound traffic
  - Software updates
  - NTP
  - DNS
- Explicitly block bogon origins
  - Even if blocked at the edge (defence in depth)

BCP38

- We should not need a slide about this in 2025!

DNS servers run DNS and nothing else

- Anything not related to DNS should not be installed
- But you must monitor your DNS installation
  - Anything you need to monitor can be installed
  - Restrict access to monitoring per best practices

DNS configuration in revision control

- See also my “Git for everyone” presentation ☺

Credential management

- No user accounts
- Restrict access to management interfaces
- Management access control with cryptographic keys or 2FA
- User access control following sound credential management

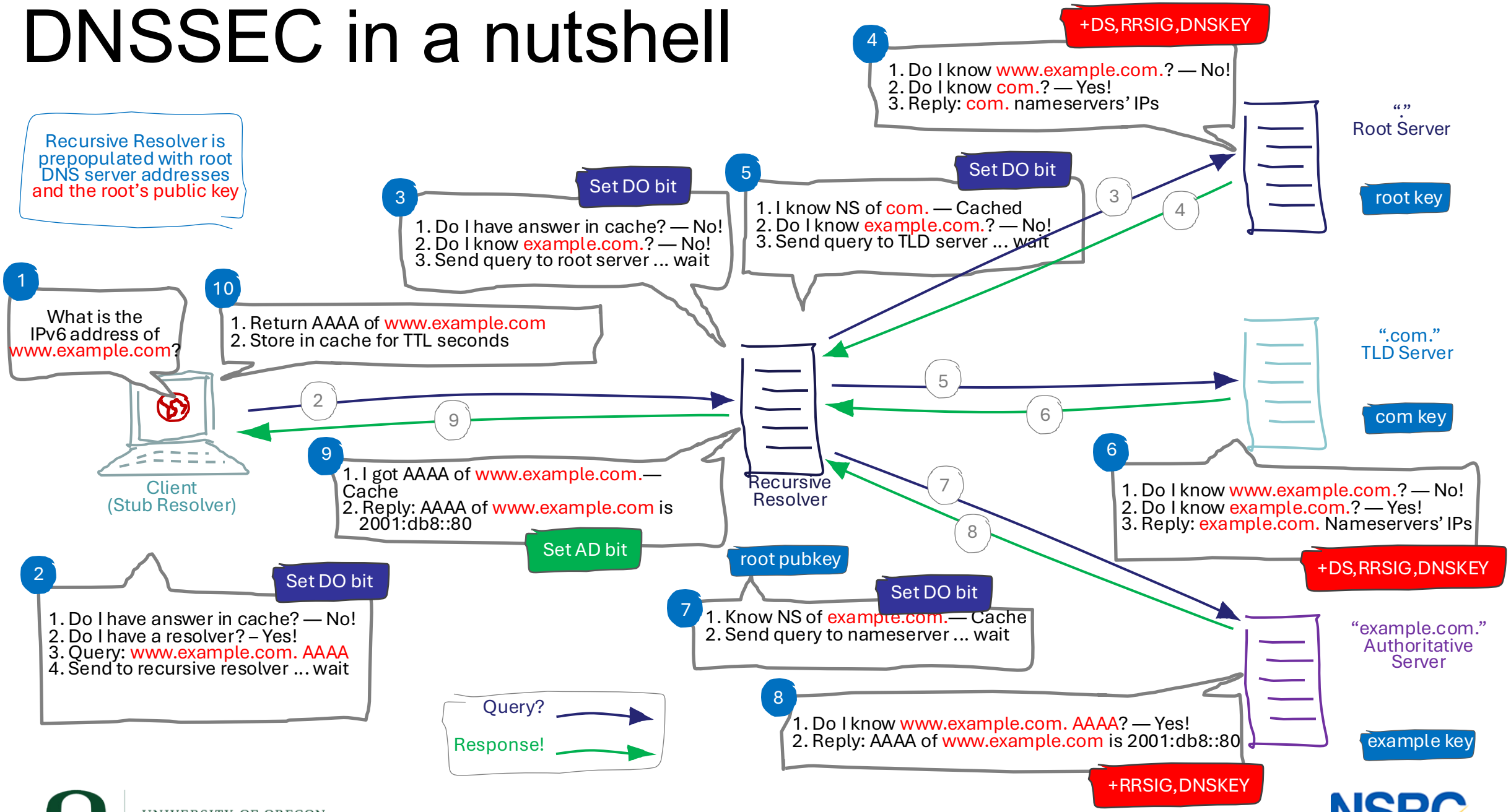
DNSSEC validation is easy – turn it on already!

RECURSIVE RESOLVER OPERATORS

Best practices

1. DNSSEC validation must be enabled
2. Restrict client access to your networks
3. QNAME minimisation must be enabled
4. Resolvers must not coexist with authoritative DNS servers
5. You must have at least two recursive resolvers
6. Monitor your DNS infrastructure
7. (Bonus) DoT and DoH should be supported

DNSSEC in a nutshell



UNIVERSITY OF OREGON

Diagram credit: Md Abdul Awal

NSRC Network Startup Resource Center

Enabling DNSSEC

- BIND: on by default
- Unbound: on by default
- PowerDNS: on by default
- Windows DNS: on by default (allegedly) (but…)

If you don’t turn it off, it will Just Work!

Enabling DNSSEC (2)

- There is no reason to turn off DNSSEC validation. Ever.

Enable QNAME minimisation

- BIND: on by default
- Unbound: on by default
- PowerDNS: on by default
- Windows DNS: no support

Cannot run KINDNS-compliant recursive DNS on Windows (but why would you want to try…?)

Availability and resilience

- Resolvers must not coexist with authoritative DNS servers
- You must have at least two recursive resolvers
- Monitor your DNS infrastructure

Software diversity

- Run different software stacks in your organisation
  - FreeBSD, Linux, Solaris,… maybe not Windows
  - BIND, NSD, Knot, PowerDNS
- A critical bug in Linux or BIND should not compromise your operations
- Remember to give each software stack equal exposure
- Automation makes things a little bit easier

Restrict access to your networks

- Don’t be an open resolver!
- ACL DNS queries at the edge if you can
- Defence in depth: drop queries on your DNS servers too

Open resolvers today… Lots!

Monitoring

- All infrastructure must be monitored
- Remember to monitor both success & failure cases
  - Test your monitoring
- Common metrics
  - Latency
  - Known-good responses
  - DNSSEC “AD” bit

Assess your operational practices and correct/adjust unaligned practices

KINDNS SELF-ASSESSMENT

KINDNS self-assessment

- Operators can enrol to participate in one or many categories covered by KINDNS
  - Participation in KINDNS means voluntarily committing to implement and adhere to agreed norms and practices
  - Participants become goodwill ambassadors and promote best practices

https://kindns.org/self-assessment/

Join the KINDNS initiative!

- KINDNS mailing list operated by ICANN: kindns-discuss@icann.org
- KINDNS wiki: https://community.icann.org/display/KINDNS