



KINDNS

An ICANN Initiative to Promote DNS Operational Best Practices

Adiel A. Akplogan

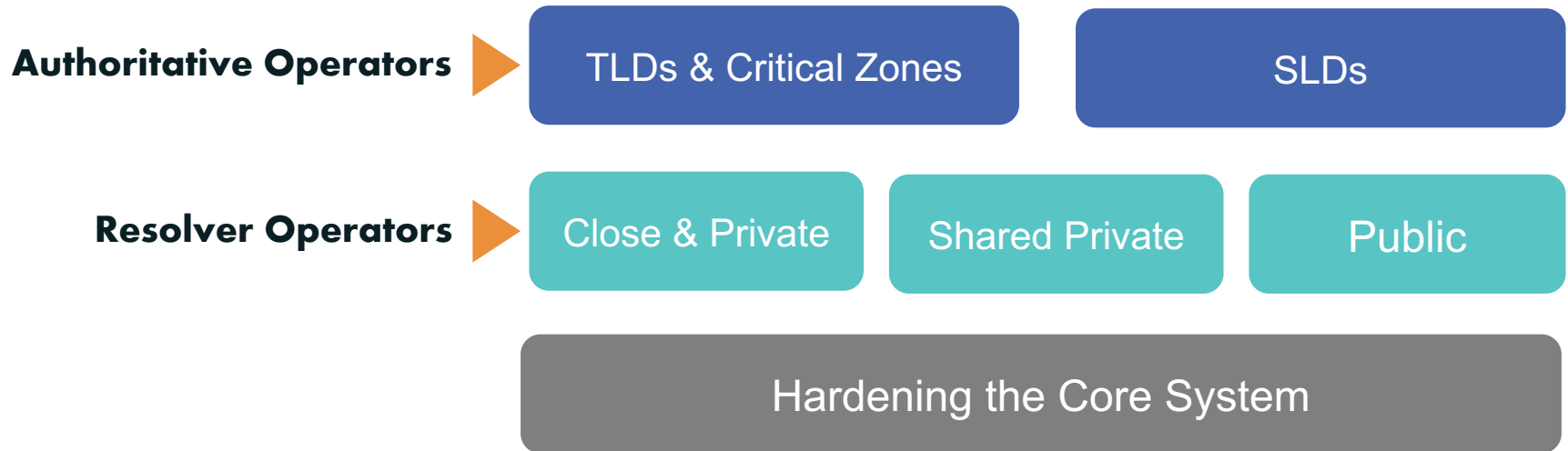
August 2022VP, Technical Engagement,
ICANN



Knowledge-sharing and
Instantiating
Norms for
DNS (Domain Name System) and
Naming
Security

..... is pronounced "kindness."

An initiative to produce something simple to refer to 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.



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

1. **MUST** be DNS Security Extensions (DNSSEC) signed and follow key management best practices.
2. Transfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. There **MUST** be diversity in the operational infrastructure: **Network, Geographical, Software**
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

SLDs

1. **MUST** be DNSSEC signed and follow key management best practices
2. Transfer between authoritative servers **MUST** be limited
3. Zone file integrity **MUST** be controlled
4. Authoritative and recursive nameservers **MUST run on separate infrastructure**
5. A minimum of two distinct nameservers **MUST** be used for any given zone
6. Authoritative servers for a given zone **MUST** run from diversified infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Private resolvers are not publicly accessible and cannot be reached over the open internet. They are typically found in corporate networks or other restricted-access networks

Closed & Private resolvers

1. DNSSEC validation **MUST** be enabled
2. Access control list (ACL) statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. Authoritative servers for a given zone **MUST** run from a diversified Infrastructure
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

Shared private resolver operators are typically ISPs or similar hosting service providers. They offer DNS resolution services to their customers (mobile, cable/DSL/fiber users, as well as hosted servers and applications).

Shared Private resolvers

1. DNSSEC validation **MUST** be enabled
2. ACL statements **MUST** be used to restrict who may send recursive queries
3. QNAME minimization **MUST** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. At least two distinct servers **MUST** be used for providing recursion services
6. The infrastructure that make up your DNS infrastructure **MUST** be monitored
7. **For privacy consideration:** Encryption (DOH or DoT) **SHOULD** be enabled
8. Private resolver operators **SHOULD** have software diversity

This category includes both open and closed public resolvers. Closed public resolvers are typically commercial DNS filtering/scrubbing services, such as DNSfilter and OpenDNS.

Shared Private resolvers

1. DNSSEC validation **MUST** be enabled
2. QNAME minimization **MUST** be enabled
3. **For** privacy considerations: Encryption (DOH or DoT) **SHOULD** be enabled
4. Authoritative and recursive nameservers **MUST** run on separate infrastructure
5. Data collected through the passive logging of DNS queries **MUST** be limited
6. At least two distinct servers **MUST** be used for providing recursion services
7. Public resolver operators **MUST** ensure operational diversity in their infrastructure.
8. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

In addition to implementing best practices for DNS security and for DNS availability and resilience, all operators must pay careful attention to practices for hardening the platforms their DNS services use.

Core Hardening

1. ACLs **MUST** be implemented to control network traffic to your DNS servers
2. BCP38/MANRS egress filtering **MUST** be implemented
3. The configuration of each DNS server **MUST** be locked down
4. User permissions and application access to system resources **MUST** be limited
5. System and service configuration files **MUST** be versioned
6. Access to management services **MUST** be restricted
7. Access to the system console **MUST** be secured using cryptographic keys and/or two factor authentication mechanism.
8. Credentials Management for customer access **MUST** adhere to best practices

1. Operators in each category can self assess their operational practices against KINDNS and use the report to correct/adjust unaligned practices.
 - Self-Assessments will be anonymous, and reports will be directly downloaded from the web site.
2. Operators can enroll to participate in one or many categories covered by KINDNS.
 - Participation in the KINDNS initiative means voluntarily committing to implement/adhere to agreed practices.
 - Participants becomes goodwill ambassadors and promote best practices.



Website – kindns.org (kindns.club)



KINDNS

Standards for Knowledge-Sharing and Instantiating Norms for DNS and Naming Security.

It's a program to develop a framework that focuses on the most important operational best practices or concrete instances of DNS security best practices.

[JOIN US](#) [SELF-ASSESSMENT](#)

Working with the DNS technical community, we've identified and documented a set of best practices that are essential for a secure DNS ecosystem, and that both small and big operators can easily implement.

Implementing KINDNS practices is voluntary. The goal of KINDNS is not to lecture operators or overwhelm them with a complex list of things to do, but rather to aid them in understanding and implementing a small set of the most important operational best practices.

KINDNS is intended as a movement, where members of the global community help themselves and each other by committing to the KINDNS best practices.

The more operators join the initiative, the larger the footprint of a robust and secure DNS ecosystem will be. By joining the KINDNS initiative, you are voluntarily committing to adhering to the mutually agreed norms and acting as "goodwill ambassadors" within the community.

[Join Us Today](#)
Support the DNS ecosystem security

[KINDNS Self-Assessment](#)
Access yourself today

Latest News

Sample Post 3
20 April 2022

Sample Post 2
19 April 2022

Sample Post 1
18 April 2022

[MORE NEWS](#)

KINDNS

Self Assessment

Home / Self Assessment

Welcome

This DNS Operators self assessment has two components:

1. Core DNS Practices Assessment
2. Core System Security Assessment

The assessment will begin as soon as you press start.

Name*

[Start ->](#)

KINDNS

Private Resolvers

Home / Private Resolvers

Private resolvers are normally found on corporate/restricted networks and are not publicly accessible. They are often located on private IP address subnets (RFC1918, for instance), limiting reachability from the rest of the internet (with or without the use of access control lists/firewalls). Private resolvers are in some cases part of a trusted computing domain (e.g., Active Directory).

There are two types of best practices for private recursive resolver operators: DNS security, and DNS availability and resilience. In addition to these two categories specific to the core DNS, all operators must pay careful attention to practices related to hardening their core system security.

DNS Security: These best practices are aimed at improving the security of your DNS service itself, helping prevent users from being served malicious data, and lowering the chances of data corruption going unnoticed.

Practice 1

DNSSEC validation **MUST** be enabled for recursive resolvers.

Rationale

Practice 2

QNAME minimization **MUST** be enabled to mitigate leakage of domain names.

Rationale

DNS Availability and Resilience: These best practices aim to improve the robustness, resilience, and stability of your DNS infrastructure. Some of the recommendations can be implemented with minimal changes or additions to your infrastructure.

Practice 3

Authoritative and recursive name servers **MUST NOT** be mixed on the same DNS infrastructure.

Rationale

Practice 4

At least two distinct servers **MUST** be used for providing recursion services.

Rationale

Practice 5

Monitoring of the services, servers, and network equipment that make up your DNS infrastructure **MUST** be implemented.

Rationale

© KINDNS 2022 All Rights Reserved / Contact / Policies / Powered by Blacklight

- ⦿ **The KINDNS discussion mailing list:**

kindns-discuss@icann.org

- ⦿ **Wiki page** where we will share preliminary documents until the formal website is developed and launched

<https://community.icann.org/display/KINDNS>

- ⦿ **The Project team:**

Adiel Akplogan	Alexandra Dans
Steven Kim	David Closson
Philippe Regnault	David Huberman
Karen Scarfone	Kinga Kowalczyk

Engage with ICANN



Thank You and Questions

Visit us at icann.org

Email: kindns-info@icann.org



[@icann](https://twitter.com/icann)



facebook.com/icannorg



youtube.com/icannnews



flickr.com/icann



linkedin/company/icann



soundcloud/icann



instagram.com/icannorg