An ICANN Initiative to Promote DNS Operational Best Practices

SAFNOG-7
Cape Town

Yazid AKANHO
Technical Engagement Senior Specialist
ICANN

KINDNS

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

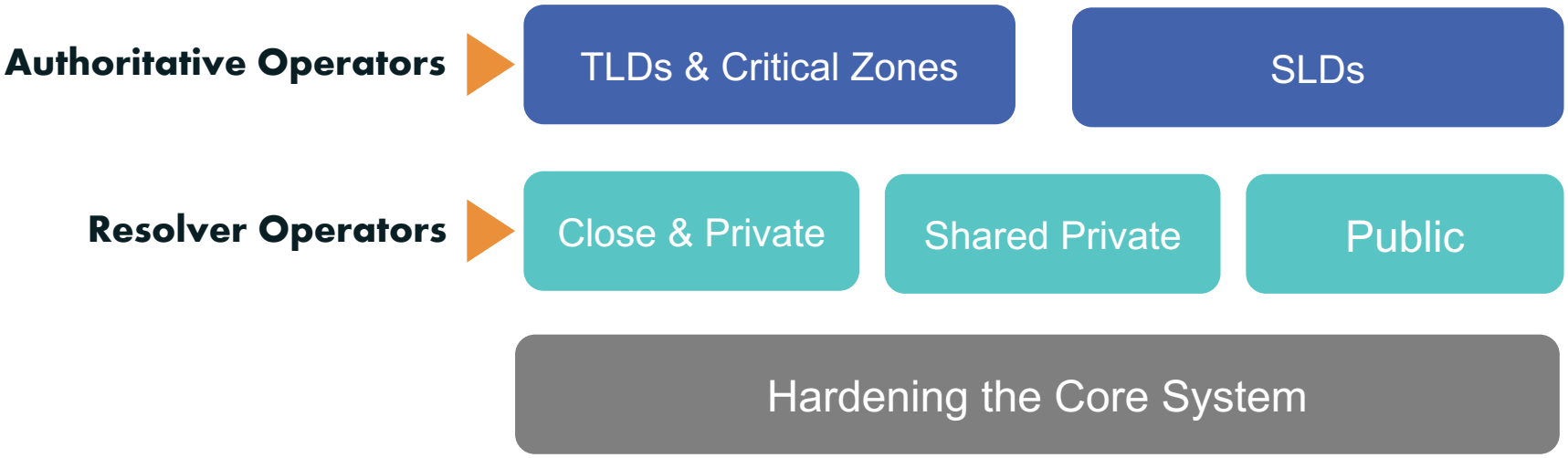
….. is pronounced ”kindness.”

What Is It?

KINDNS

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.

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.

Authoritative DNS Operators of Critical Zones

KINDNS

TLDs & Critical Zones

1. **MUST** be DNS Security Extensions (DNSSEC) signed and follow key management best practices.
2. **T**ransfer 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

Authoritative DNS Operators of SLDs

KINDNS

SLDs

1. **MUST** be DNSSEC signed and follow key management best practices
2. **T**ransfer 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

Closed & Private Resolver Operators

KINDNS

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

KINDNS

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 pr**ivacy consideration: Encryption (DOH or DoT) **SHOULD** be enabled
8. Private resolver operators **SHOULD** have software diversity

Public Resolver Operators

KINDNS

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

Hardening the Core

KINDNS

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

Self Assessment & Enrollment

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.

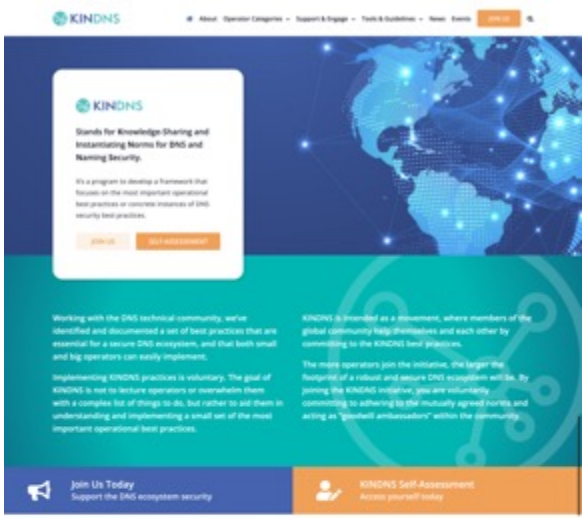
   - Participation in the KINDNS initiative means voluntarily committing to implement/adhere to agreed practices.
   - Participants becomes goodwill ambassadors and promote best practices.

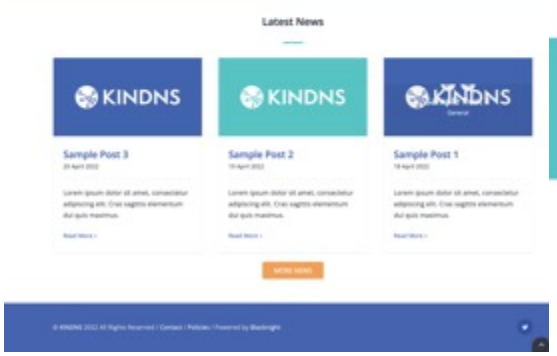
Self-Assessment Report

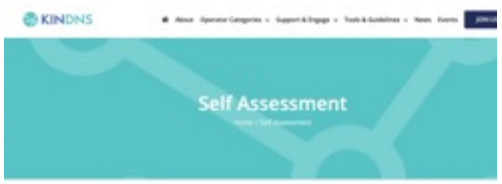
KINDNS

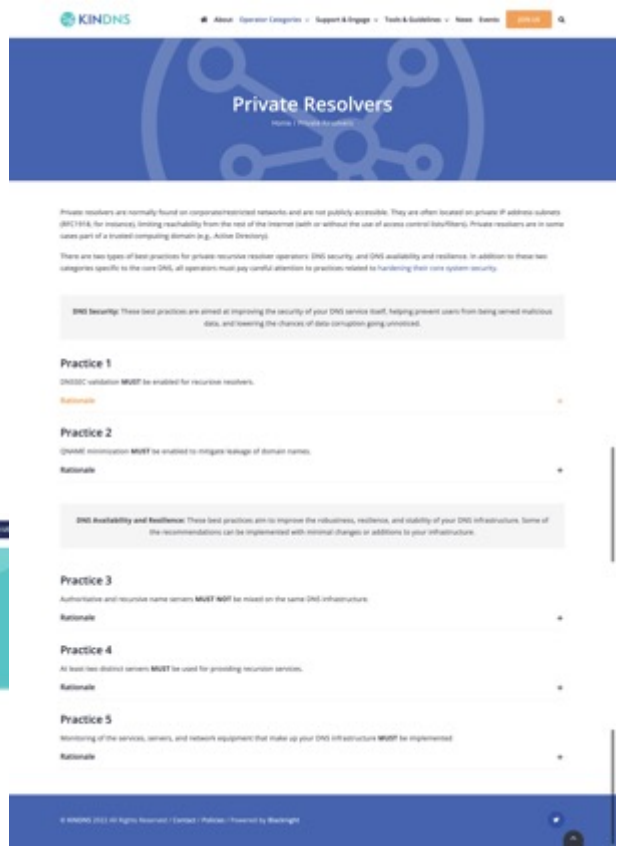
Website – kindns.org (kindns.club)

KINDNS





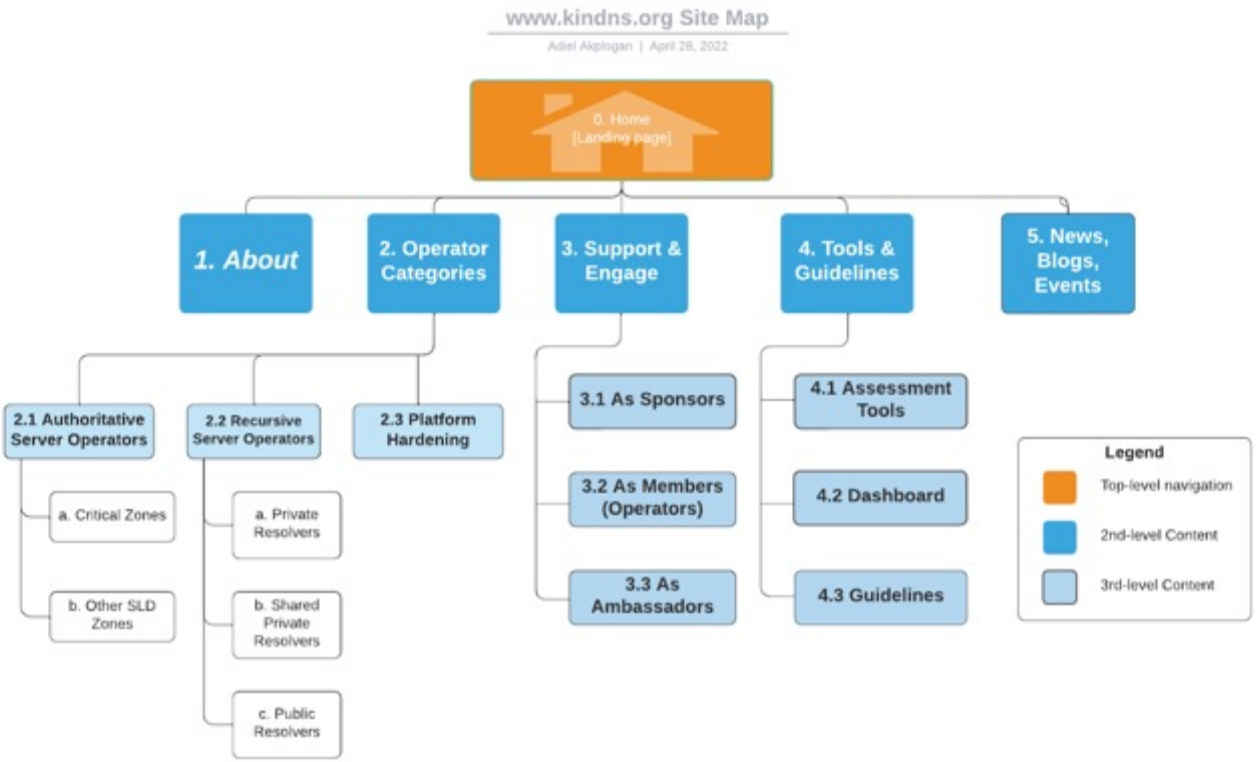




Website Map

KINDNS

kindns.org



How to Stay Informed and Contribute

- **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


facebook.com/icannorg


youtube.com/icannnews


flickr.com/icann


linkedin/company/icann


soundcloud/icann


instagram.com/icannorg