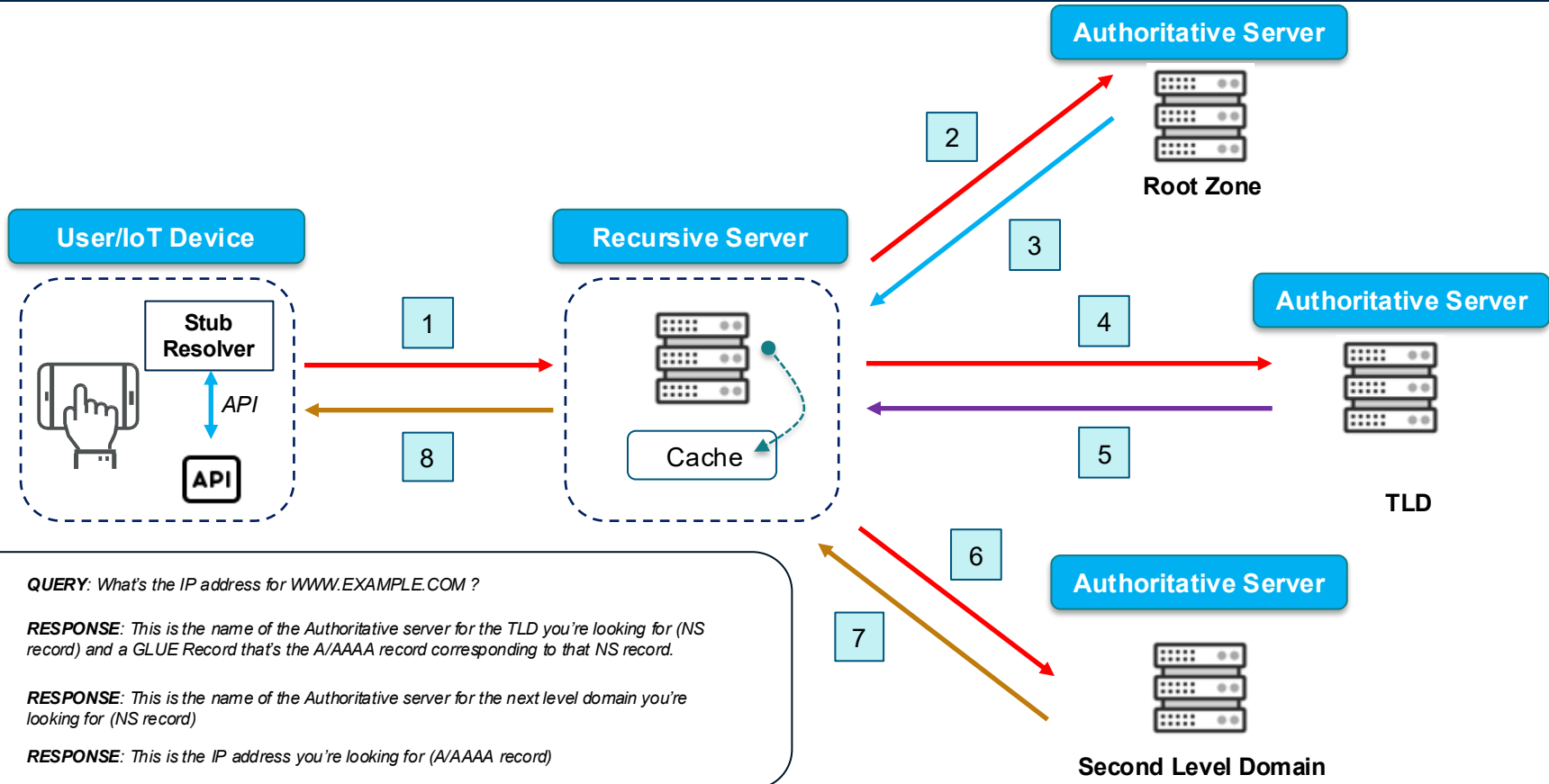




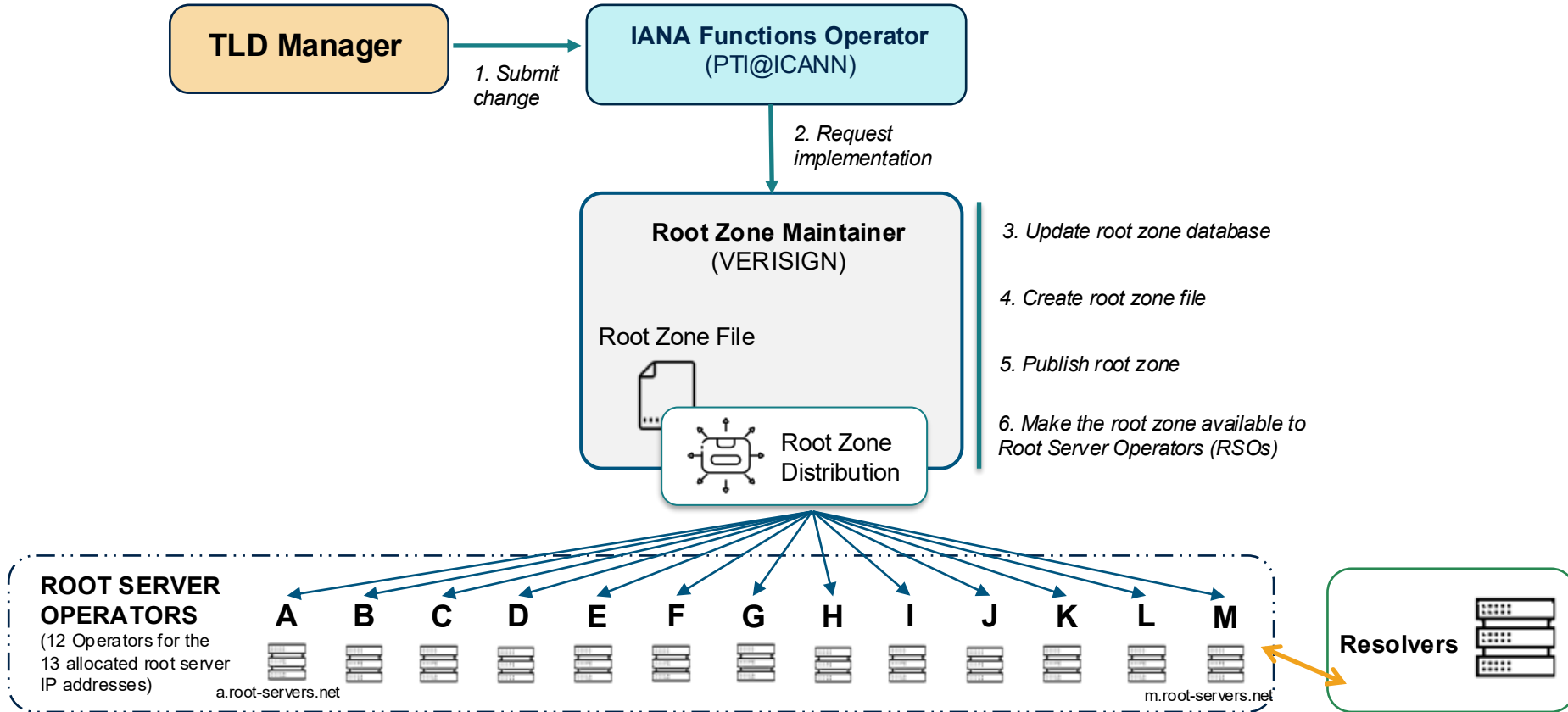
# Promoting DNS Operational and Security Best Practices

Champika Wijayatunga <[champika.wijayatunga@icann.org](mailto:champika.wijayatunga@icann.org)>

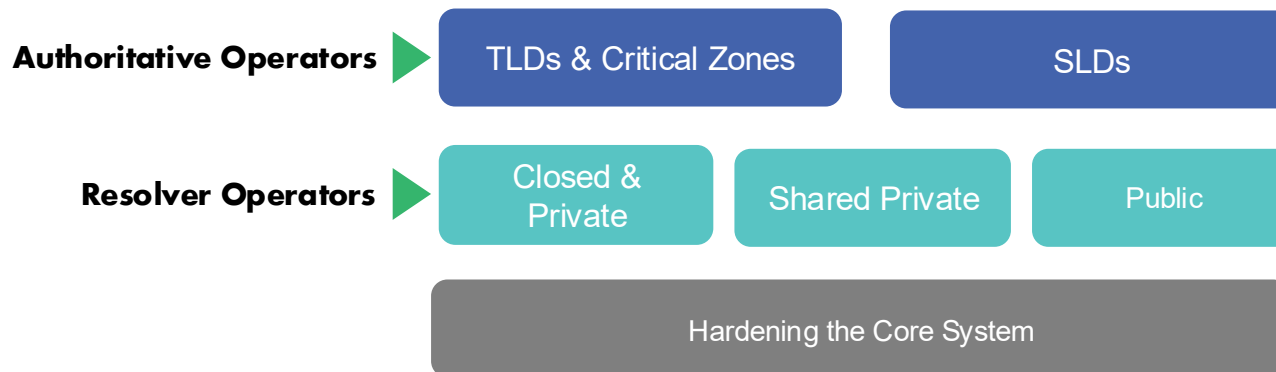
# DNS Query Resolution



# Root Zone Management



# 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.

# Best Practices for Authoritative DNS Operators

- DNSSEC signing
- Key management best practices
- Zone Transfers between authoritative servers need to be limited
- Zone file integrity
- Run the authoritative and recursive nameservers on separate infrastructure
- A minimum of two distinct nameservers for any given zone
- Authoritative servers for a given zone should run from a diversified infrastructure
- Diversity in the authoritative DNS software packages
- DNS Monitoring

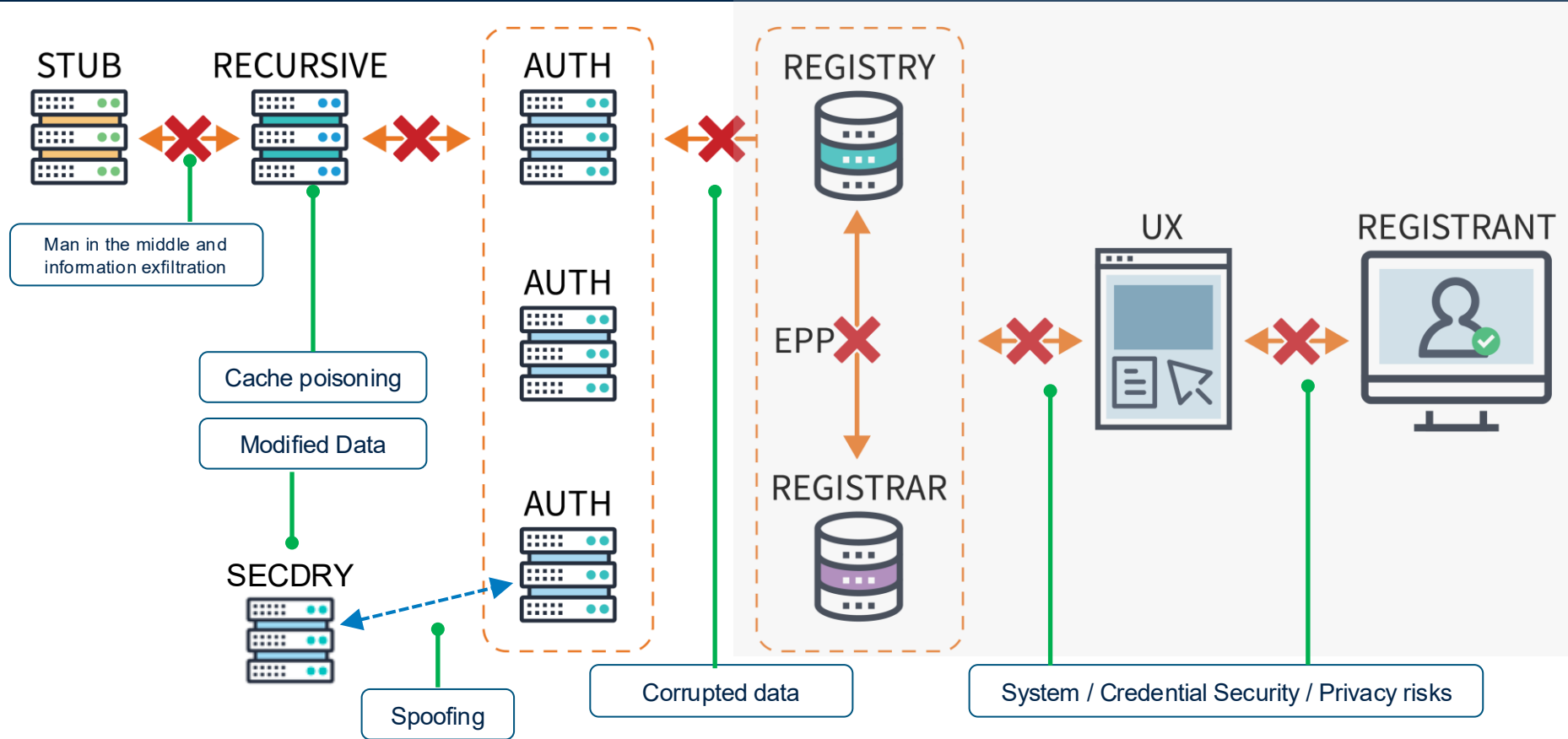
# Best Practices for Recursive DNS Operators

- Enable DNSSEC validation
- Access Controls to restrict who may send recursive queries
- Enable QNAME minimization
- Run the authoritative and recursive nameservers on separate infrastructure
- At least two distinct servers for providing recursion services
- Diversity in the recursive DNS software packages
- Recursive servers to run from a diversified Infrastructure
- DNS Monitoring
- For privacy consideration: encryption (DoH or DoT) can be enabled

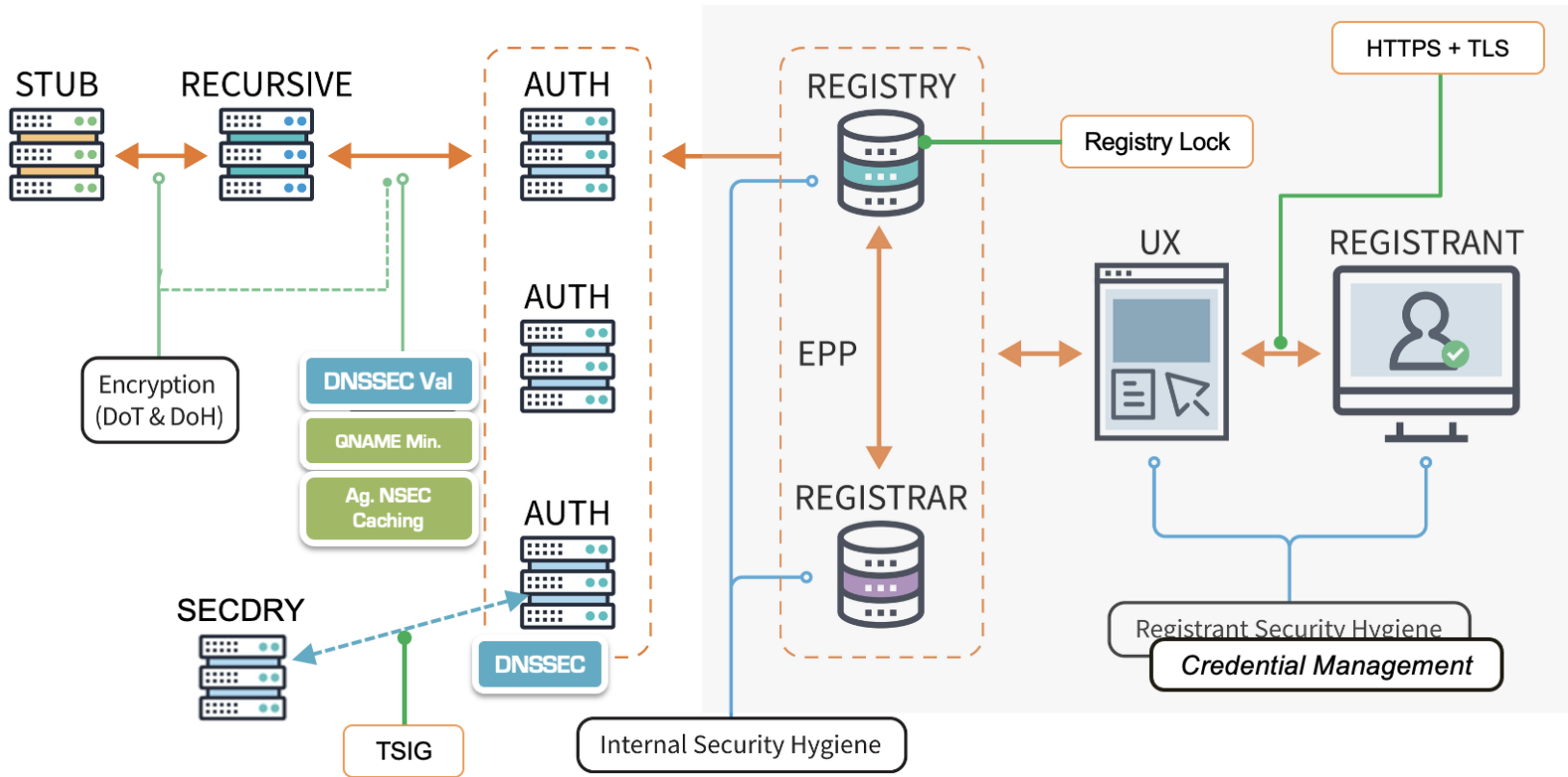
# Hardening the Core

- ACLs can be implemented to control network traffic to your DNS servers
- Access controls on DNS server configurations, management services etc.
- BCP38/MANRS egress filtering should be implemented
- Version controls on system and service configuration files
- Access to the system console should be secured using cryptographic keys and/or a multi-factor authentication mechanisms
- Credentials for customer access must offer two-factor authentication

# Potential Target Points of the DNS Infrastructure

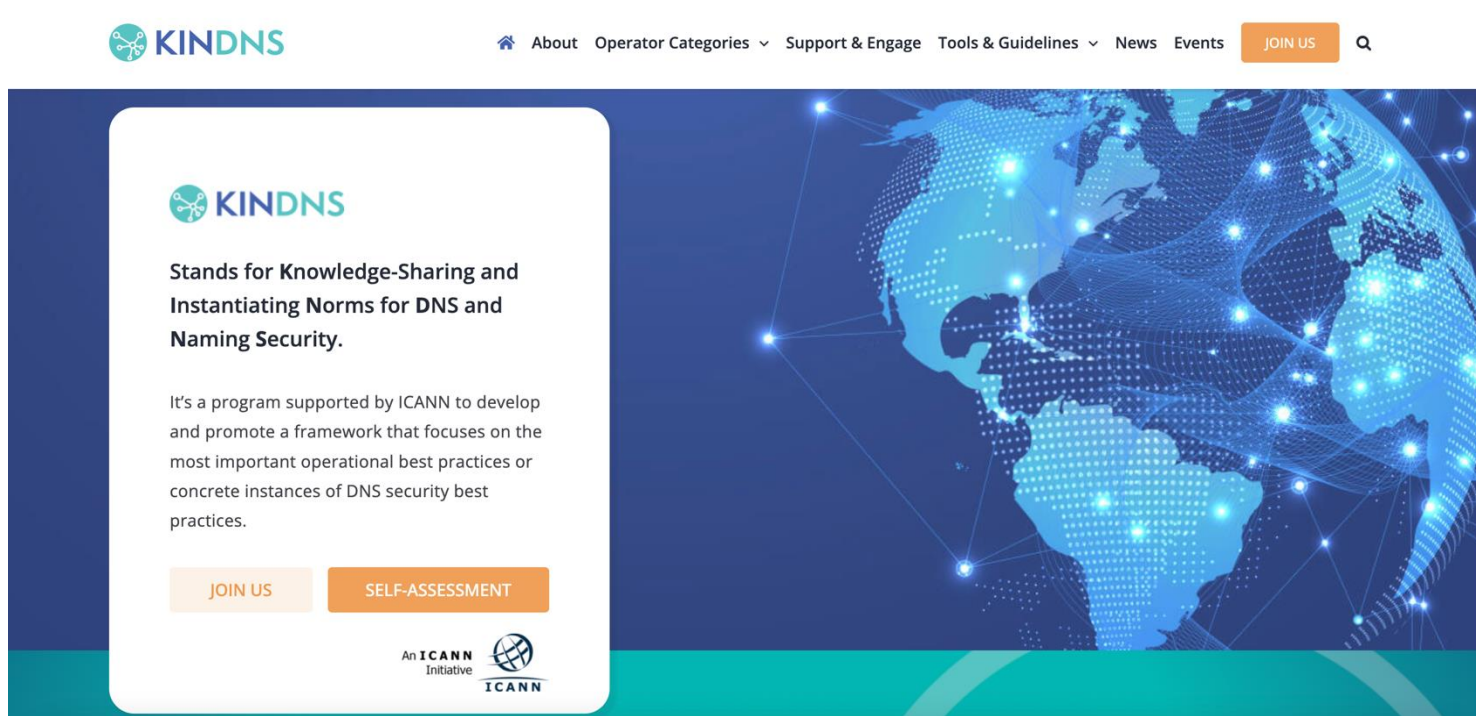


# Securing the DNS Infrastructure



# Follow KINDNS guidelines

- [www.kindns.org](http://www.kindns.org)



**KINDNS**


About Operator Categories Support & Engage Tools & Guidelines News Events [JOIN US](#)

**KINDNS**

**Stands for Knowledge-Sharing and Instantiating Norms for DNS and Naming Security.**

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

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

An ICANN Initiative 

# Engage with ICANN – Thank You and Questions



One World, One Internet

Visit us at [icann.org](https://icann.org)

Email: [champika.wijayatunga@icann.org](mailto:champika.wijayatunga@icann.org)



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



[facebook.com/icannorg](https://facebook.com/icannorg)



[youtube.com/icannnews](https://youtube.com/icannnews)



[flickr.com/icann](https://flickr.com/icann)



[linkedin/company/icann](https://linkedin/company/icann)



[slideshare/icannpresentations](https://slideshare/icannpresentations)



[soundcloud/icann](https://soundcloud/icann)