

DNSSEC

•Ulrich Wisser, Technical Engagement Manager, Europe
ulrich.wisser@icann.org

•October 2026

Security by DNS

KINDNS

Security by DNS

EMAIL

KINDNS

Security by DNS

SPF

DKIM

DMARC

KINDNS

DANE

Security by DNS

PRIVACY

KINDNS

Security by DNS

TLS

KINDNS

50% of all TLS certificates are issued by Let's Encrypt

HOW ARE THEY VERIFIED?

Security by DNS

DNS

KINDNS

How do you designate a specific CA for your domains?

Security by DNS

DNS

KINDNS

Security for DNS



KINDNS

Security for DNS

DNSSEC

KINDNS

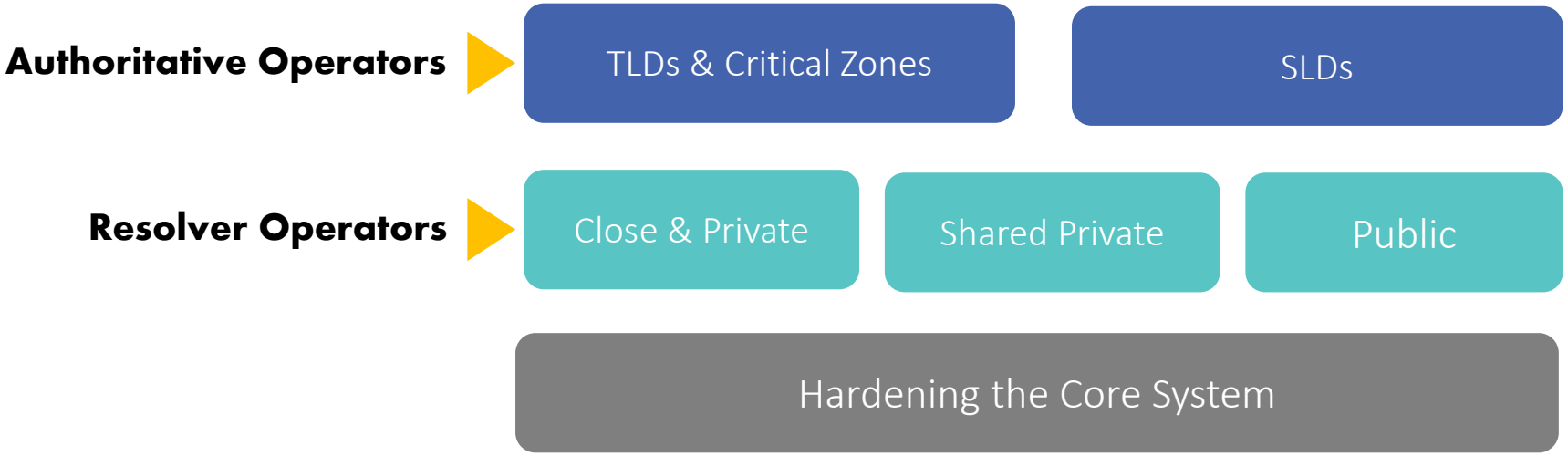


KINDNS

KINDNS

An Initiative to Promote DNS Operational Best Practices

Targeted Operators



- Each category has 6-8 practices that we will encourage operators to implement. See www.kindns.org, for more details
- By joining KINDNS, DNS operators are voluntarily committing to adhere to these identified practices and act as "goodwill ambassadors" within the community.

KINDNS

Hardening the Core

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

KINDNS

Authoritative DNS Operators of Critical Zones

TLDs & Critical Zones

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. There **MUST** be diversity in the operational infrastructure: **Network, Geographical, Software**
7. The infrastructure that makes up your DNS infrastructure **MUST** be monitored

KINDNS

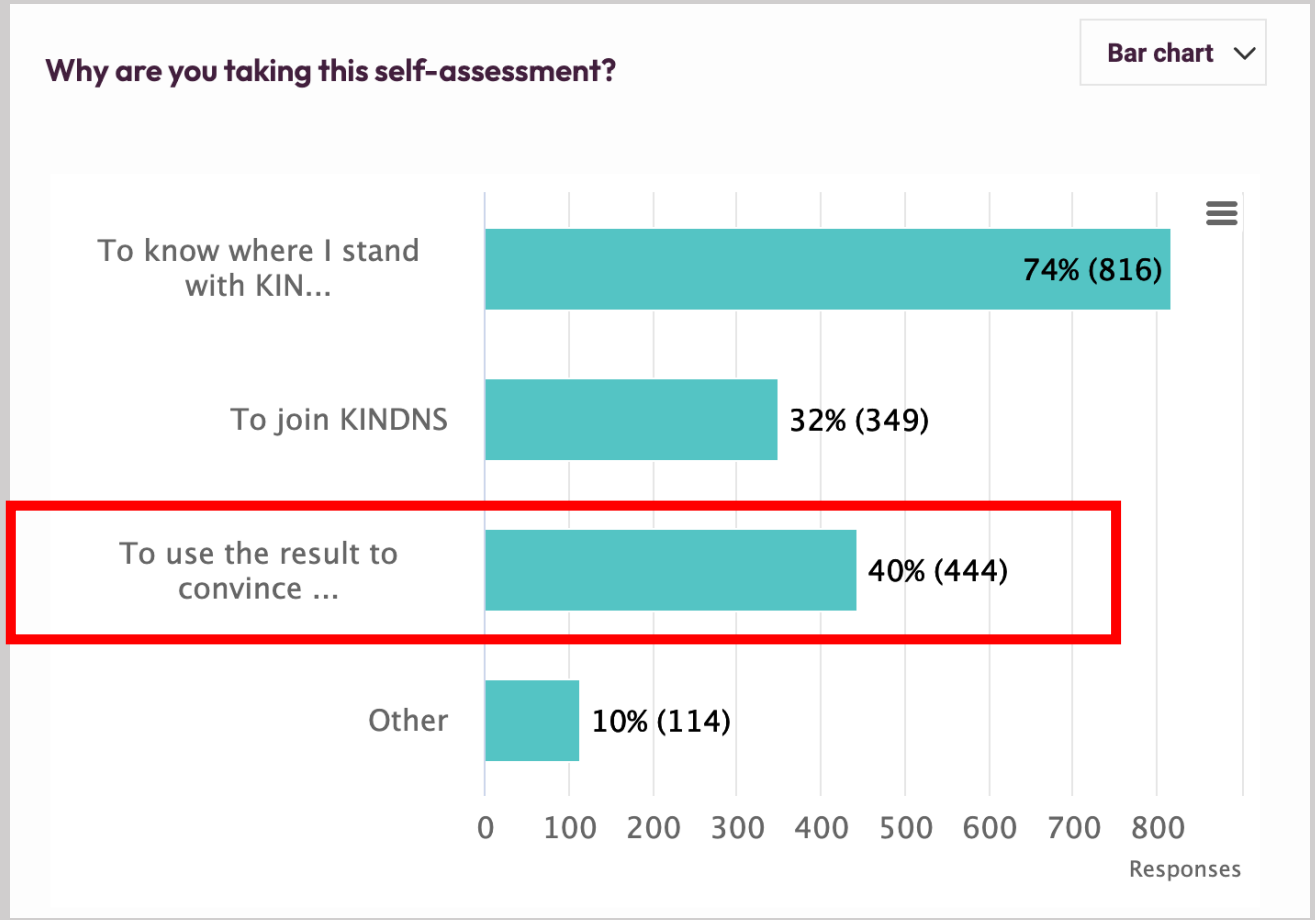
Shared Private Resolvers

Shared private resolver operators are typically ISPs or similar hosting service providers. They offer DNS resolution services to their customers. These resolvers are normally shared between many different customers.

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 makes up your DNS infrastructure **MUST** be monitored
7. DoT (DNS-over-TLS) or DoH (DNS-over-HTTPS) **SHOULD** be enabled

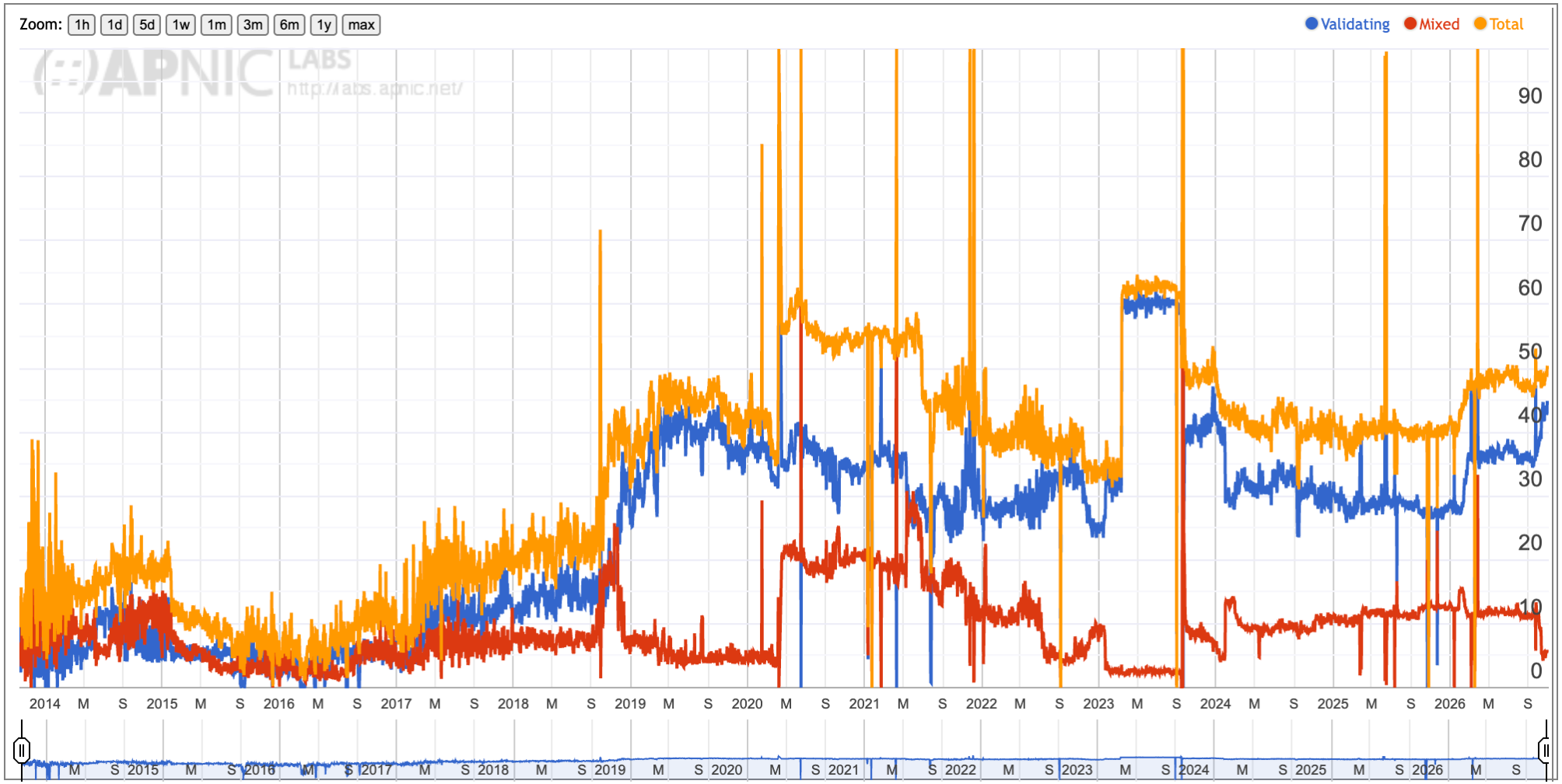
KINDNS


Why are you taking this self-assessment?
Bar chart
To know where I stand with KIN...
74% (816)
To join KINDNS
32% (349)
To use the result to convince ...
40% (444)
Other
10% (114)
0
100
200
300
400
500
600
700
800
Responses

DNSSEC Statistics

KINDNS

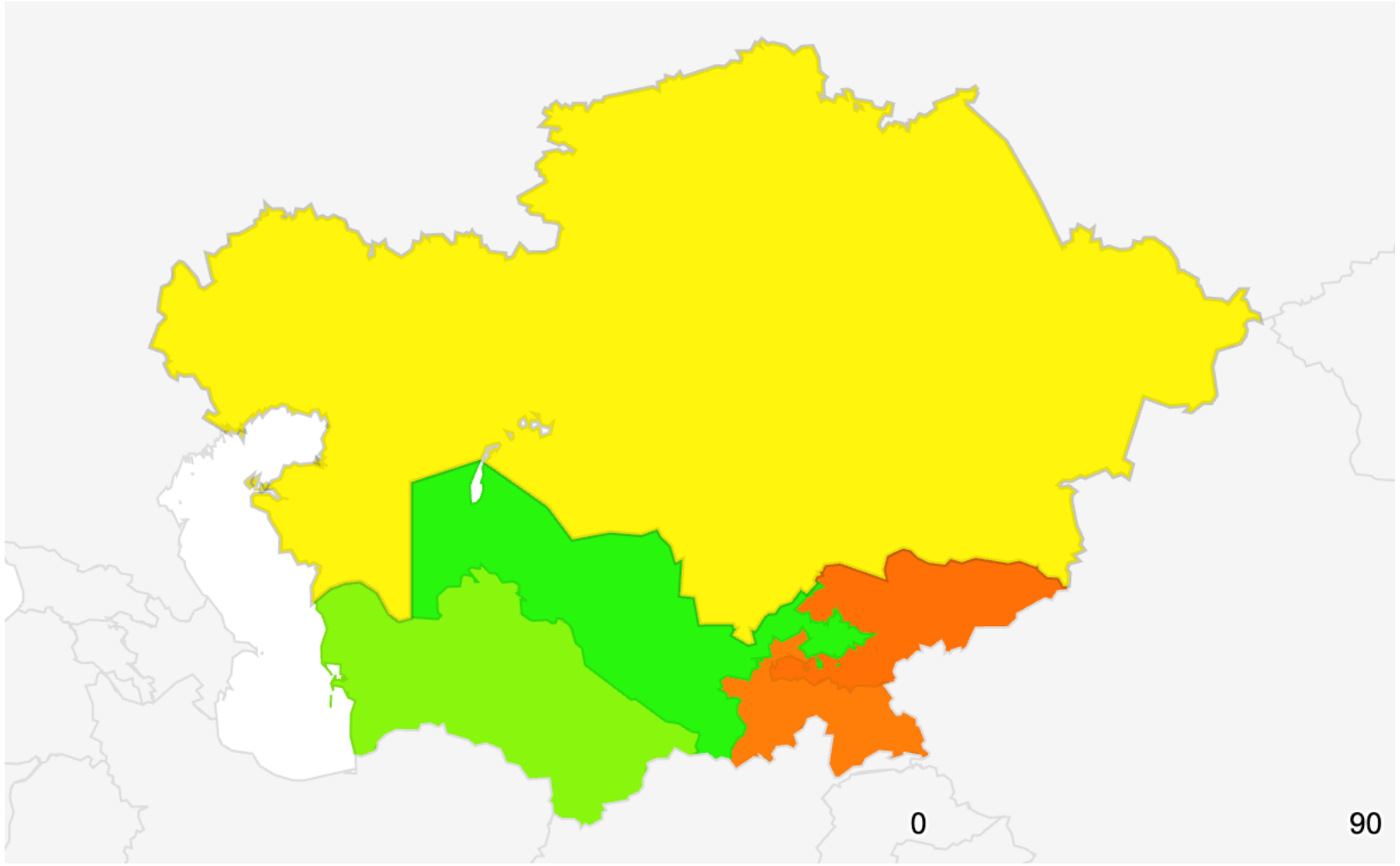
Use of DNSSEC Validation for Kazakhstan



Source: APNIC Labs https://stats.labs.apnic.net/dnssec/KZ

KINDNS

Use of DNSSEC Validation for Central Asia



Source: APNIC Labs https://stats.labs.apnic.net/dnssec/XR

KINDNS

Stay Informed and Contribute



Website	www.kindns.org
Twitter	https://twitter.com/4KINDNS
E-Mail	info@kindns.org
Mailing list	kindns-discuss@icann.org

KINDNS