ccTLD.UA With XoT

Hostmaster.UA
2025-06-09
ICANN83 Praha

UA ccTLD Timeline, 2011-2023

2011-12-02 UA RSA KSK (UADOM 2011)

2012-03-27 UA zone signed, algoritm 10

2012-04-13 UA DS in root

2019-10-29 Generated ECDSA KSK

2019-11-07 IANA: Root DS updated

2023-11-15 Knot migration, UA SLDs

2025, Time of a Change (again)

We are using Knot code and BIND cloud

Automatic ZSK management

Zone incremental updates are minimal

Distribution layer: feed to 6 anycasts*

Why Knot?

What are the benefits of Knot signer?

Can rotate ZSK by schedule

ZSK do not overlap in time

RRSIG generated only when needed

NSEC3 salt auto-updated (magic -1 *)

Very small IXFR updates possible

CZNIC provided valuable support

Why BIND?

What are the benefits of BIND anycast?

Stable code, feature rich, documented

Existing complex configuration

ISC provides support contracts(*)

Why XoT?

What are the benefits of XFR over TLS?

Protection against eavesdropping

Authentication of both sides of XFR

Can be used together with TSIG

No large overhead (octets on wire)

Recently modern standard (RFC 9103)

How?

How we have done it

Start small: one zone, one server pair

Tested Knot primary to BIND secondary

Also tested Knot to Knot

All configuration changes tracked in Git

Currently all zones use it (signer to distribution and then to service layer)

Lessons

Lessons learned as we go

There are too many variables

Not every configuration was tested yet

We are not ready to use CA chain validation yet, especially with third parties

NOTIFY and AXFR TLS use can differ(*)

BIND logging is not comprehensive

Takeaways

Set small goals

Have a backup plan

Know how to reach developers*

Don’t be afraid to fail — but fix fast!

Ask industry experts then become one

and...

DON’T PANIC!

Thanks

IETF for DNS

ISC for BIND

CZNIC for Knot

Rcode0 for deployment insights

My team for working while war continues

Contacts

Dmytro Kohmanyuk

dk@cctld.ua

dnssec@hostmaster.ua

https://hostmaster.ua/dnssec