

# Automated DNSSEC

Ulrich Wisser  
Technical Engagement Manager, Europe

May 2025



# Security by DNS

---

# DNS as Trust Anchor

---

# EMAIL

---

# SPAM

---

**SPF**  
**DKIM**  
**DMARC**

---

# DANE

---

# TLS



---

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

---

# How are they verified?

---

# DNS

# Security for DNS

---

# DNSSEC

# Signing your domain

# Signing

example.com.	300	IN	A	127.0.0.1
example.com.	300	IN	A	127.0.1.1
example.com.	300	IN	A	127.1.1.1
example.com.	300	IN	<b>RRSIG</b>	A 13 2 300
	<b>20221103191825</b>		20221020174825	12345
	gtdS0mpgFKzZAYw4FfBOHkhVHrS3cLZFU...==			

---

# DNSSEC Problems

- Needs constant refresh of data (signatures)  
SOLVED with modern name server software



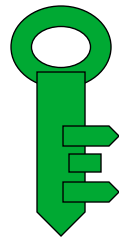
# Chain of Trust



.COM



AUTHENTICATES



EXAMPLE.COM

---

# DS Records

example.com.            300   IN        **DS** 31406    13            2  
                         F78CF3344F72137235098ECBBD08947...

# DNSSEC Problems

- Needs constant refresh of data (signatures)  
SOLVED with modern name server software
- Needs to sync with parent on key introduction/roll-over  
SOLVED but not widely implemented (yet)

# RFC 8078 - Managing DS Records from the Parent via CDS/CDNSKEY

- A child zones publishes CDS / CDNSKEY records
- CDS has exactly the same format as DS RR
- CDNSKEY has exactly same format as DNSKEY RR
- The parent zone (or other parties who can change the zone) scan actively for CDS / CDNSKEY (at the child apex)
- The parent zone gets updated with a new DS RRset

# RFC 9615 - Automatic DNSSEC Bootstrapping Using Authenticated Signals from the Zone's Operator

- CDS and/or CDNSKEY record(s) are published in the zone of the name server
- E.g. example.com has two name servers ns1.example.net, ns2.example.net
- Publish
  - \_dsboot.example.com.\_signal.ns1.example.net. CDS ...
  - \_dsboot.example.com.\_signal.ns2.example.net. CDS ...

# RFC 7477 - Child-to-Parent Synchronization in DNS

- A child zones publishes CSYNC records
- The parent zone or other parties who can change the zone scan actively for CSYNC (at the child apex)
- The parent zone gets updated with a new RRset

# Updating policy

RFC 8078 gives several different ways of doing this  
Most common so for “Accept after Delay”

## DS in parent: NO

several vantage points  
use TCP/IP  
same results over several  
3 days

## DS in parent: YES

several vantage points  
correctly signed

Make sure domain stays resolvable with new DS record(s)

# Knot DNS Configuration

## remote

- id: quad9  
address: 9.9.9.9

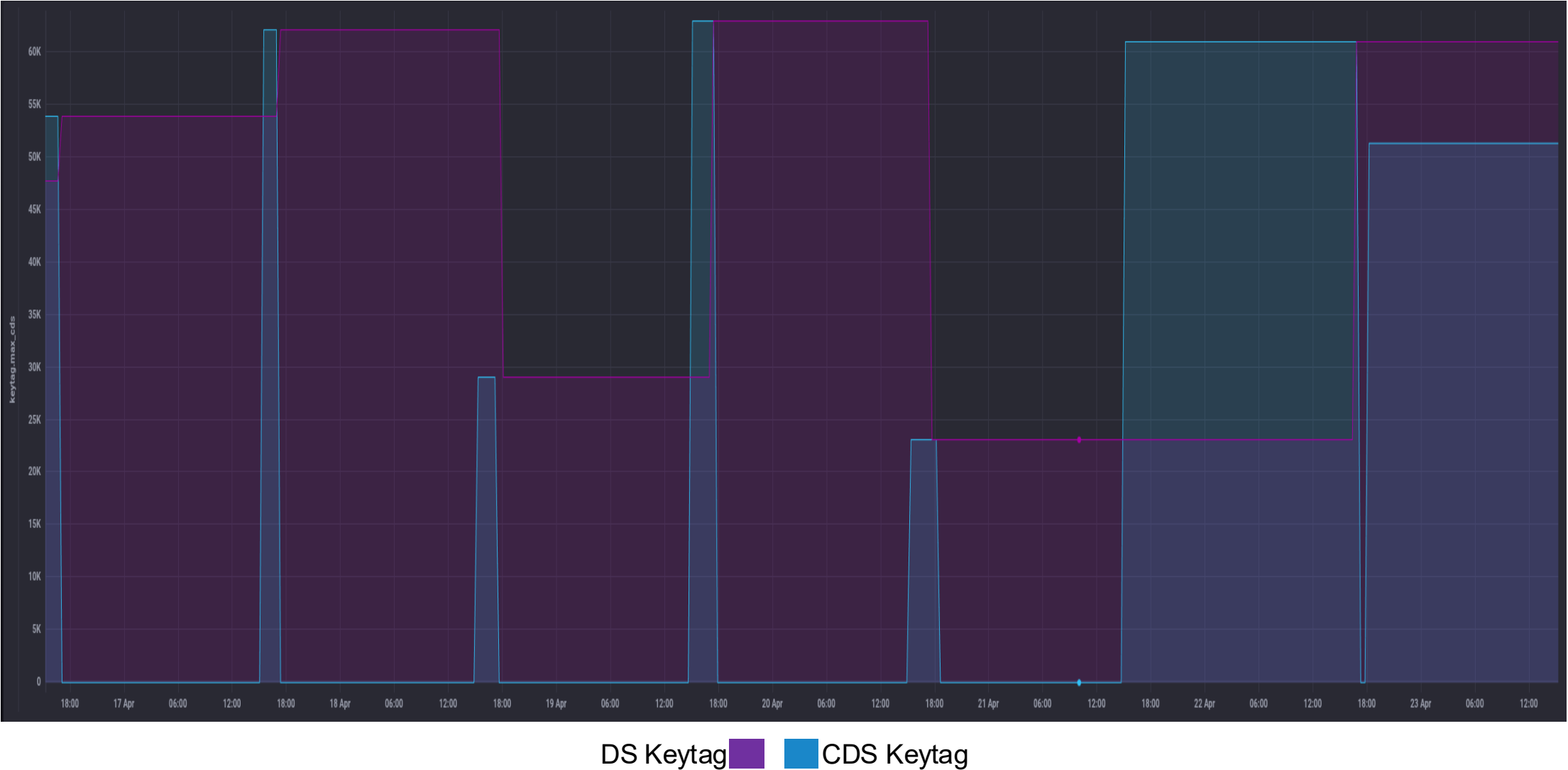
## submission:

- id: quad9  
check-interval: 30m  
parent: quad9

## policy:

- id: **insane**  
zsk-lifetime: 4h  
ksk-lifetime: 24h  
ksk-submission: quad9  
algorithm: ecdsap256sha256  
propagation-delay: 1m  
dnskey-ttl: 3m  
zone-max-ttl: 5m  
cds-cdnskey-publish: rollover  
rrsig-lifetime: 1h  
rrsig-refresh: 5m  
rrsig-pre-refresh: 1m  
reproducible-signing: on  
nsec3: off  
cds-digest-type: sha256  
dnskey-management: full  
delete-delay: 30s






# Trouble Shooting


## Query domain


Search for a domain name ending with either ".se" or ".nu" in the input field and hit search to see the status.

Any dates presented are in UTC.

If any error occurred during the scanning process you can retrieve more information about the error by testing the domain name in our testing tool [Zonemaster](#).



Logs 

 JSON

Domain	tysk.se
Status	Done = The scanning process has completed successfully.
FirstValidAt	2025-04-23 14:34:48
LastValidAt	2025-04-23 14:34:48

---

# Who can run a scanner?

- ccTLDs operate under their own rules  
These rules decide if the registry can update domains and deploy dnssec automation
- gTLDs are under contract with ICANN  
gTLDs can not update domain information  
registrars can deploy dnssec automation

---

# DRAFT - Generalized DNS Notifications

<https://datatracker.ietf.org/doc/draft-ietf-dnsop-generalized-notify/>

- Parent publishes a DSYNC record
- DSYNC record specifies where to send a notify
- Child sends notify to initiate scan

# Security and Stability Advisory Committee (SSAC)

## **SAC126 DNSSEC Delegation Signer (DS) Record Automation**

<https://itp.cdn.icann.org/en/files/security-and-stability-advisory-committee-ssac-reports/sac-126-16-08-2024-en.pdf>

# RFC 7477 - Child-to-Parent Synchronization in DNS

- A child zones publishes CSYNC records
- The parent zone or other parties who can change the zone scan actively for CSYNC (at the child apex)
- The parent zone gets updated with a new RRset

# RFC 8590 - Change Poll Extension for the Extensible Provisioning Protocol (EPP)

<https://www.rfc-editor.org/rfc/rfc8590.html>

- Allows registries to notify registrars of any changes the registry might have made to an object in its database.

# Additional Resources

---

## List of implementations

By Ondřej Caletka (Ripe NCC)

<https://github.com/oskar456/cds-updates>

## DNSSEC Deployment map

(formerly ISOC now at George Mason University)

<https://maps.dnssec.gmu.edu/>





# ONE WORLD, ONE INTERNET

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