Automated DNSSEC

Ulrich Wisser
Technical Engagement Manager, Europe

February 2025

Security by DNS

EMAIL

SPF
DKIM
DMARC
DANE

DNS

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

How are they verfied?

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 **RRSIG** A 13 2 300

20221103191825 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 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	DS in parent: YES
several vantage points use TCP/IP same results over several 3 days	several vantage points correctly signed

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

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

DRAFT - Automating DNS Delegation Management via DDNS

https://datatracker.ietf.org/doc/draft-johani-dnsop-delegation-mgmt-via-ddns/

- Builds on ”Generalized DNS Notifications”
- Defines a new scheme
- Updates get signed with a SIG(0) signature
- Describes method for bootstrapping

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

ONE WORLD, ONE INTERNET

Visit us at **icann.org**


@icann


facebook.com/icannorg


youtube.com/icannnews


flickr.com/icann


linkedin/company/icann


slideshare/icannpresentations


soundcloud/icann