RIPE NCC
RIPE NETWORK COORDINATION CENTRE

DNSSEC

Florian Obser | NONOG-4 | 2022-09-21

About me

- Senior system engineer
  - k.root-servers.net (AS25152)
  - AuthDNS (AS197000)
    - pri.authdns.ripe.net
    - f-reverse
    - ripe.net
    - Various ccTLDs
- OpenBSD developer
  - author of unwind(8)
    - validating resolver, based on unbound

About DNS

- Globally distributed, scalable, hierarchical database
- Everything on the Internet uses it for federation
  - Visiting a website
  - Sending an Email
  - Requesting a TLS certificate
  - “Forgot my password” links

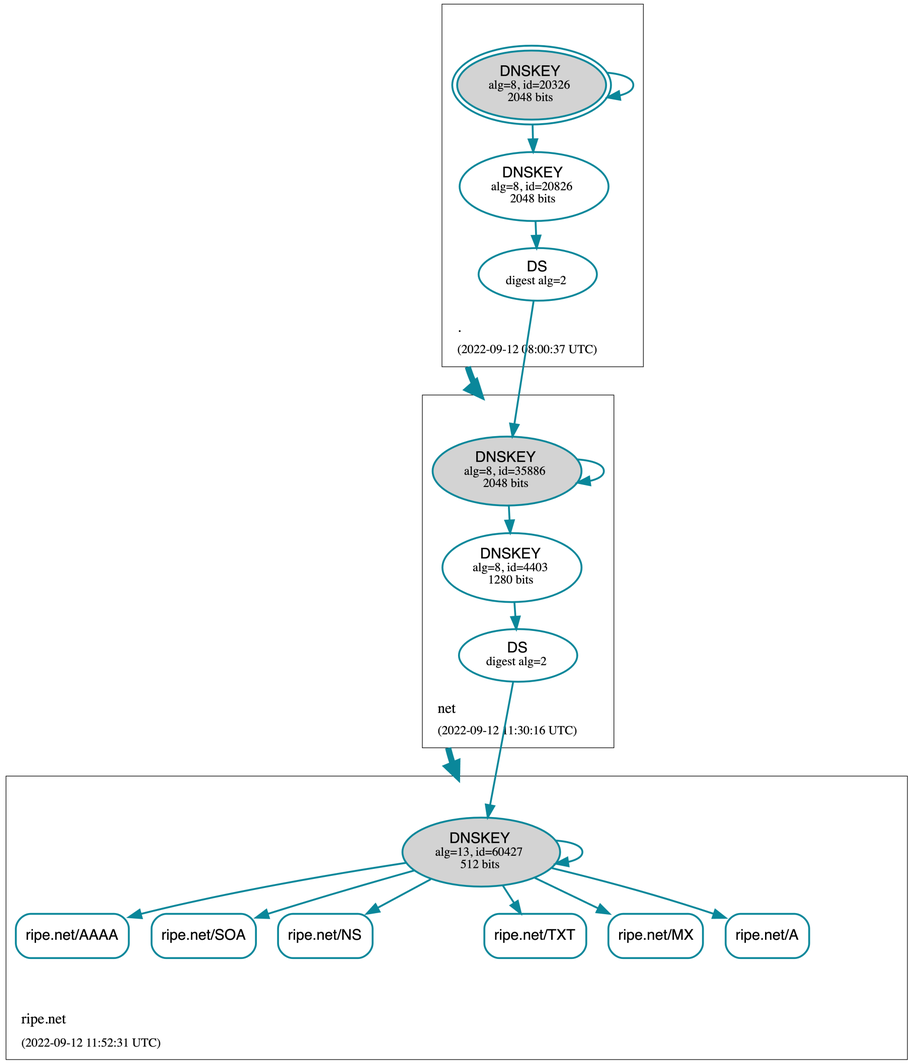
Problems with DNS

- No data integrity
- No authenticated data origin
- No authenticated denial of existence
- No privacy / confidentiality
  - Not this talk

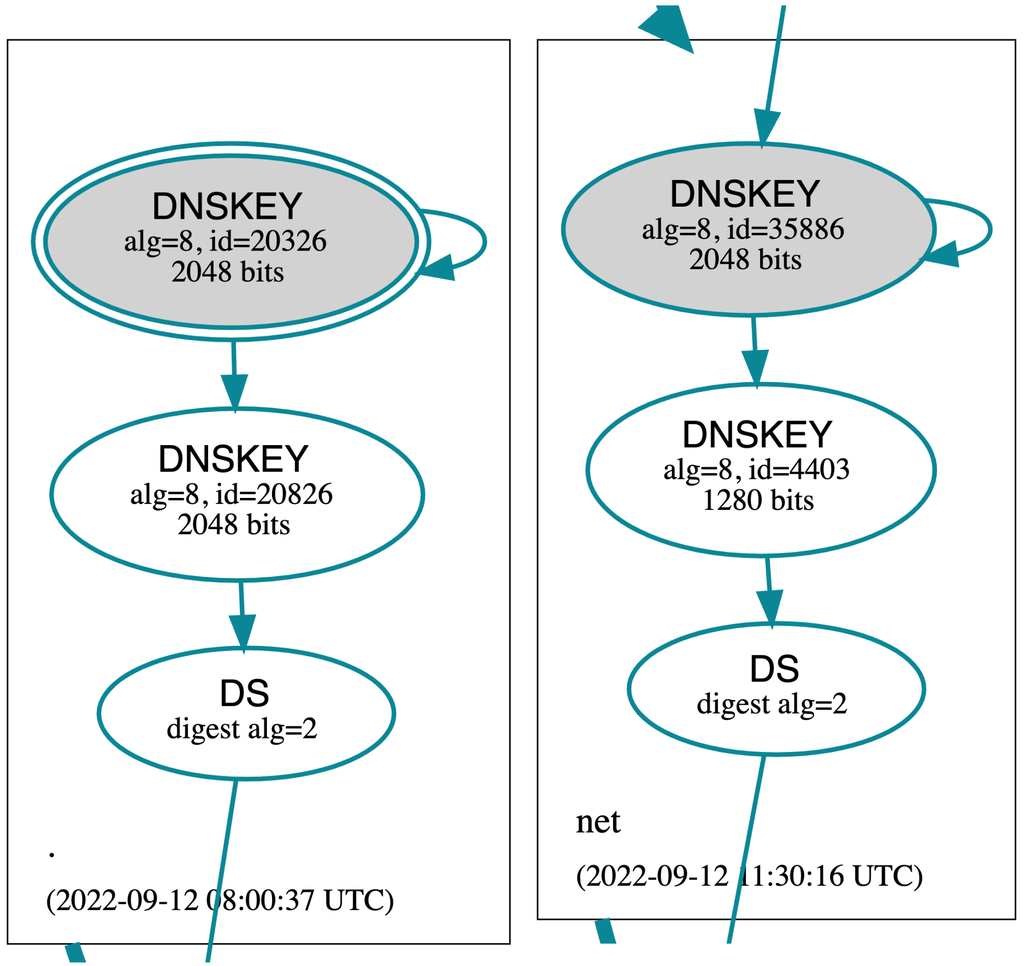
DNSSEC

- Public-key cryptography (DNSKEY)
- Signatures over authoritative data (RRSIG)
- Well known trust-anchor
  - Key Signing Key of the root zone
- Delegate cryptographic authority (DS)
- Signing on zone change or RRSIG expiry, not per query

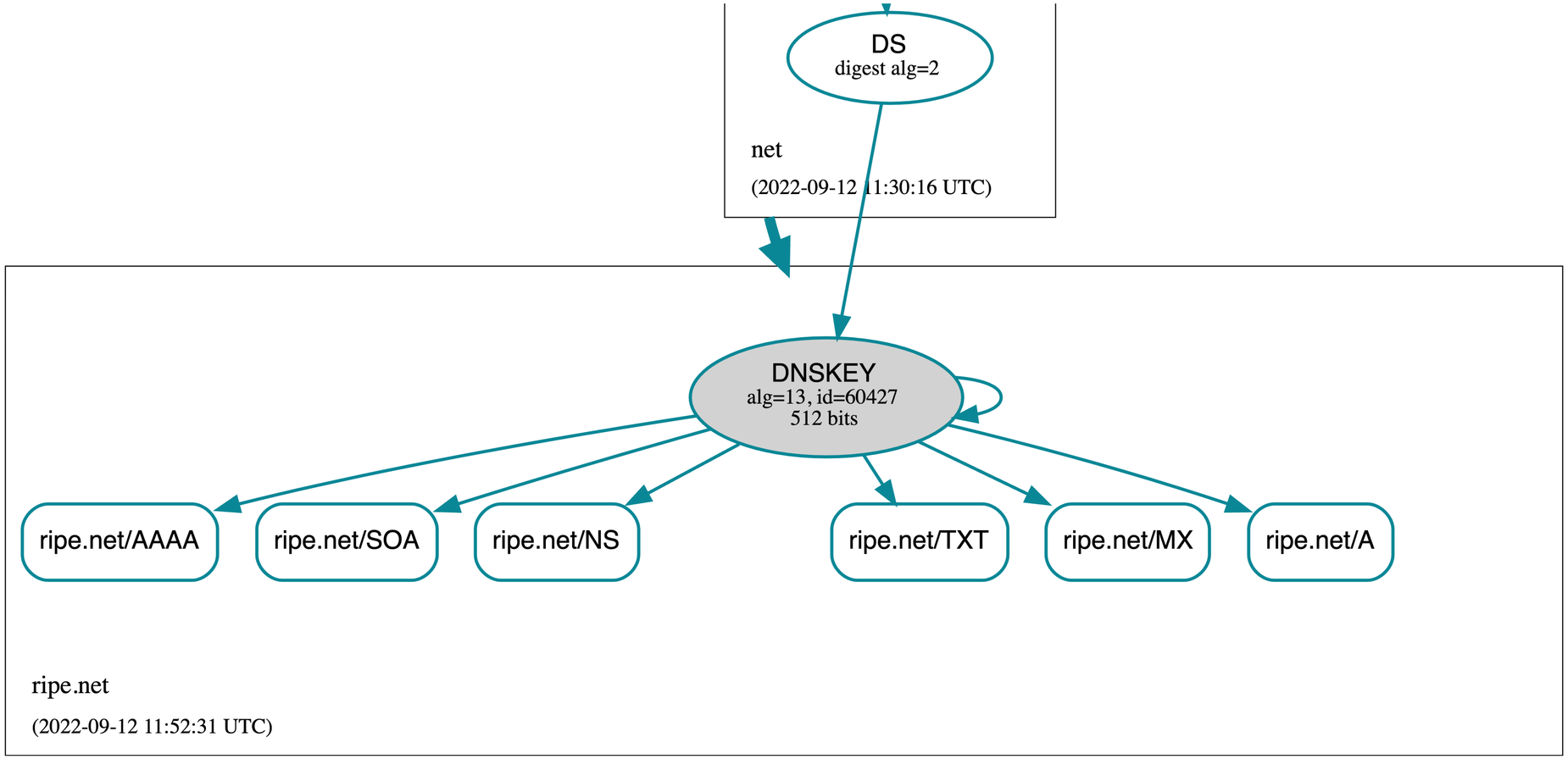
DNSViz - ripe.net



DNSViz - root and .net



DNSViz - ripe.net



DNSSEC Operations

- General DNS hygiene
  - No lame delegations
  - Keep name servers in sync
- Time
  - Synchronised clocks on signers & validators
  - TTLs
    - Usually long in parent zones, ~ 1+ days in TLDs
- RRSIG expiration
    - Align RRSIG expiration with expire time in SOA record

Large answers

- IP Fragmentation
  - DNS Flag Day 2020: limit UDP answers to 1232 bytes
- Amplification attacks
  - Response Rate Limiting (RRL)
  - Elliptic curves signatures are smaller than RSA
  - NSEC answers are smaller than NSEC3 answers

Signing considerations

- ECDSAP256SHA256 (13) or RSASHA256 (8)
  - RFC 8624: Algorithm Implementation Requirements and Usage Guidance for DNSSEC
- KSK/ZSK vs. CSK
  - KSK / ZSK
    - KSK can be offline
    - (Emergency) ZSK rollovers are faster
  - CSK
    - Zone is smaller
    - Fewer moving parts if keys are online anyway
    - Rollovers need to interact with parent zone

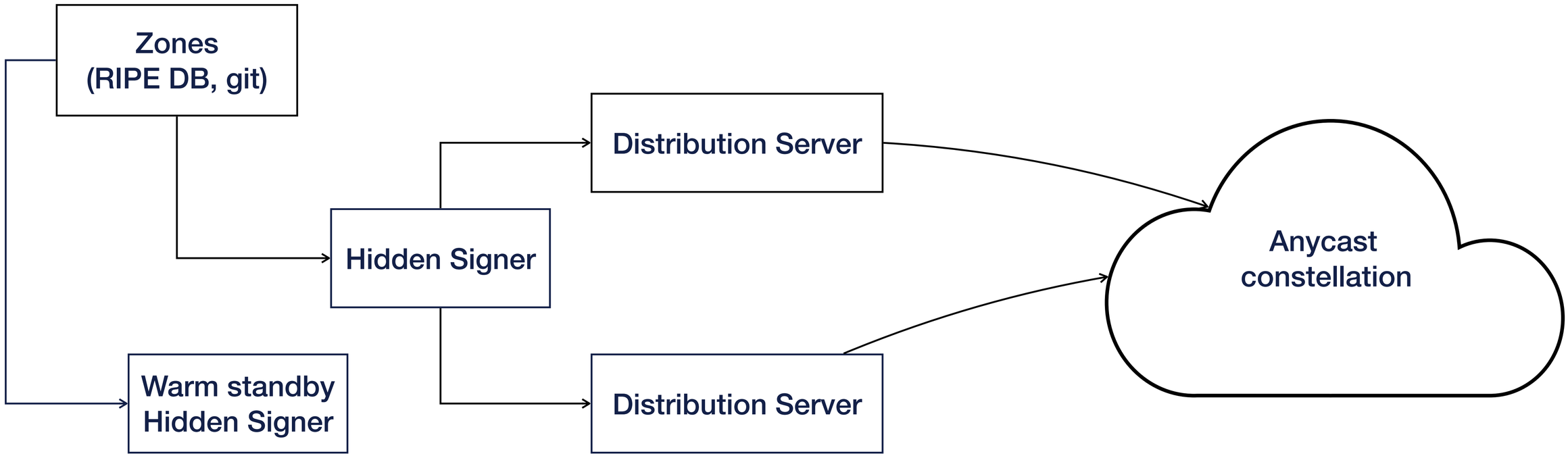
NSEC vs. NSEC3 vs. white-lies

- Provides authenticated denial of existence
- DNS records for “nothing exists in this interval”
- NSEC: labels are in the clear
  - trivial zone enumeration
- NSEC3: labels are hashed
  - susceptible to offline dictionary attacks
- white-lies: minimal interval is calculated per query
  - Requires online, per-query signing
  - Nothing is learned about zone contents

DNSSEC signing

- ~~Fiendishly clever perl one-liner~~
- FOSS (alphabetical order)
  - BIND
  - Knot DNS
  - OpenDNSSEC
  - PowerDNS

AuthDNS design



Enabling DNSSEC

- Add DS record to parent zone
  - Manual at the registrar
  - API
  - Inline using CDS / CDNSKEY

Debugging DNSSEC

- Step away from the computer and panic
- Online tools
  - dnsviz.net
  - dnssec-analyzer.verisignlabs.com
- cli tools
  - dig +dnssec +multiline +nocrypto
  - delv
- DNS-OARC
  - dns-operations mailing list
  - Mattermost server

Validation

- All public quad-x resolvers validate
- FOSS (alphabetical order)
  - BIND
  - Knot Resolver
  - PowerDNS recursor
  - Unbound

Validator operations

- Time
  - Synchronised clocks
    - Make sure NTP does not depend on DNSSEC
- Monitor SERVFAIL rate
- Be prepared to put Negative Trust Anchors (NTA) in place
- Make sure middle boxes don’t interfere

Questions?

fobser@ripe.net
@florian@bsd.network