DNSSEC

CDBUG
Sept 8th 2015
Patrick Muldoon

Overview

- Review of DNS
- What is DNSSEC
- Concepts
- Implementation

DNS Review

- Maps Hostname to IP (and IP to hostname)
- Two Types of Servers
  - Authoritative
  - Recursive

Authoritative Are where we create records, and provide the Answers
Recursive / Caching are used to lookup and store the answers from the Authoritative so that the system can scale.. (figures out who to ask and what to ask)

Authority

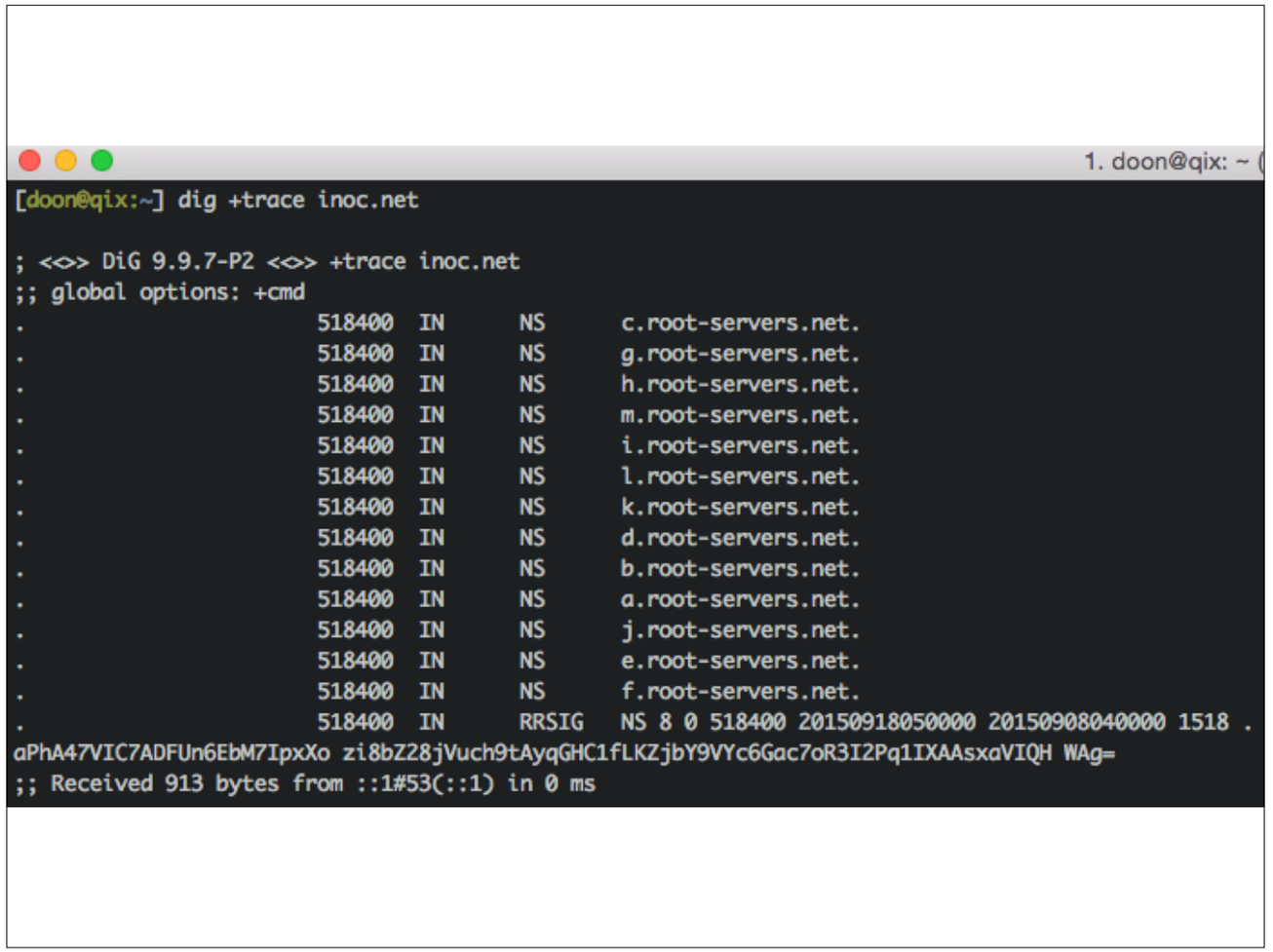
- DNS is Tree Based
- Start with (.) Root Zone and work left
- . goes to the root Servers
- net. goes to the GTLD Server
- inoc.net goes to the Auth Servers that are listed

CS tree, the root is at the top ….

```
[doon@qix:~] drill @c.gtld-servers.net ns0.inoc.net
;; ->>HEADER<<- opcode: QUERY, rcode: NOERROR, id: 35498
;; flags: qr rd ; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 6
;; QUESTION SECTION:
;; ns0.inoc.net.        IN      A

;; ANSWER SECTION:

;; AUTHORITY SECTION:
inoc.net.       172800  IN      NS      ns0.inoc.net.
inoc.net.       172800  IN      NS      ns1.inoc.net.
inoc.net.       172800  IN      NS      ns2.inoc.net.

;; ADDITIONAL SECTION:
ns0.inoc.net.   172800  IN      AAAA    2607:f058:110::a
ns0.inoc.net.   172800  IN      A       64.22.32.10
ns1.inoc.net.   172800  IN      A       199.233.228.34
ns1.inoc.net.   172800  IN      AAAA    2607:fc50:1:500::a
ns2.inoc.net.   172800  IN      A       199.48.133.234
ns2.inoc.net.   172800  IN      AAAA    2607:fc50:1000:8a00::a

;; Query time: 12 msec
;; SERVER: 192.26.92.30
;; WHEN: Tue Sep  8 11:43:38 2015
;; MSG SIZE  rcvd: 212
```

Glue Records

Lets Walk Through


1. doon@qix: ~ (
[doon@qix:~] dig +trace inoc.net
; <<>> DiG 9.9.7-P2 <<>> +trace inoc.net
;; global options: +cmd
. 518400 IN NS c.root-servers.net.
. 518400 IN NS g.root-servers.net.
. 518400 IN NS h.root-servers.net.
. 518400 IN NS m.root-servers.net.
. 518400 IN NS i.root-servers.net.
. 518400 IN NS l.root-servers.net.
. 518400 IN NS k.root-servers.net.
. 518400 IN NS d.root-servers.net.
. 518400 IN NS b.root-servers.net.
. 518400 IN NS a.root-servers.net.
. 518400 IN NS j.root-servers.net.
. 518400 IN NS e.root-servers.net.
. 518400 IN NS f.root-servers.net.
. 518400 IN RRSIG NS 8 0 518400 20150918050000 20150908040000 1518 .
aPhA47VIC7ADFUn6EbM7IpxXo zi8bZ28jVuch9tAyqGHC1fLKZjbY9VYc6Gac7oR3I2Pq1IXAAsxaVIQH WAg=
;; Received 913 bytes from ::1#53(::1) in 0 ms

```
net.                    172800  IN      NS      d.gtld-servers.net.
net.                    172800  IN      NS      k.gtld-servers.net.
net.                    172800  IN      NS      e.gtld-servers.net.
net.                    172800  IN      NS      f.gtld-servers.net.
net.                    172800  IN      NS      j.gtld-servers.net.
net.                    172800  IN      NS      h.gtld-servers.net.
net.                    172800  IN      NS      b.gtld-servers.net.
net.                    172800  IN      NS      a.gtld-servers.net.
net.                    172800  IN      NS      c.gtld-servers.net.
net.                    172800  IN      NS      l.gtld-servers.net.
net.                    172800  IN      NS      g.gtld-servers.net.
net.                    172800  IN      NS      m.gtld-servers.net.
net.                    172800  IN      NS      i.gtld-servers.net.
net.                    86400   IN      DS      35886 8 2 7862B27F5F516EBE19680444
net.                    86400   IN      RRSIG   DS 8 1 86400 20150918050000 201509
w8NvsQH0yHaa6qYeFCrTXck7 CmkbAg0NoxAad08/0rjIe7YcqR4mmn6eC+RN9N+RbBNUg0keHsoRWHMA
;; Received 729 bytes from 202.12.27.33#53(m.root-servers.net) in 90 ms
```

```
inoc.net.               172800  IN      NS      ns0.inoc.net.
inoc.net.               172800  IN      NS      ns1.inoc.net.
inoc.net.               172800  IN      NS      ns2.inoc.net.
A1RT98BS5QGC9NFI51S9HCI47ULJG6JH.net. 86400 IN NSEC3 1 1 0 - A1RUUFFJKCT2Q54F
A1RT98BS5QGC9NFI51S9HCI47ULJG6JH.net. 86400 IN RRSIG NSEC3 8 2 86400 20150913
RB24BdFu4jbEX7lFQNzgqAahBuWHqjzuBJE/ fUQBUVGsrXxBFfzZl8v+hlPXc9RKySgJi8dnu1HD
LVCJO63JQOHTSSRR1J65KFKUK1FEGRK1.net. 86400 IN NSEC3 1 1 0 - LVDQJ36ULR491FKF
LVCJO63JQOHTSSRR1J65KFKUK1FEGRK1.net. 86400 IN RRSIG NSEC3 8 2 86400 20150912
U/UpDq0+EFikF4pIdO5Y2MDS9HzNF6l1/0pM c7NPLRNS5PCHgbAbdwjX+f6fzNgRCFk7056DfMLJ
;; Received 708 bytes from 192.43.172.30#53(i.gtld-servers.net) in 83 ms
```

```
inoc.net.               3600    IN      A       64.22.32.144
inoc.net.               86400   IN      NS      ns0.inoc.net.
inoc.net.               86400   IN      NS      ns1.inoc.net.
inoc.net.               86400   IN      NS      ns2.inoc.net.
;; Received 239 bytes from 2607:fc50:1:500::a#53(ns1.inoc.net) in 22 ms

[doon@qix:~] 
```

What is DNSSEC

- Standard Public/Private Key Crypto
- Adds Cryptographic Extensions / Signatures
- Defined in RFC 4033, 4034,4035

Why is it “important”

- DNS primarily uses UDP, so any packet that comes back could be the answer
- Just needs right source and destination IPs, destination port, Query ID, and Bailiwick Check
- TL;DR — Easy to spoof

Bailiwick check is when resolvers determine which extra information in the response to ignore, Normally this is things that our out of zone of the responding server..

Commonly called cache Poisoning.

DNSSEC Fixes This

- Applies Cryptographic Check to each answer in resolution
- Can still Try to cache poison, but since they don't have the corrects keys the resolver will reject them
- Doesn't Fix (D)DOS against DNS

Concepts

Authoritative

- Zone Signing
- Rollover

Authoritative

- Sign Zone with DNSSEC Records
  - RRSIG - Signatures for A, AAAA, MX, NS, … (Tracks type/number)
  - NSEC/NSEC3 — Used for Confirming NXDomain
  - DNSKEY — Public Keys for Entire Zone
  - DS Record — Given to Parent Zone to authenticate NS records

Zone Signing

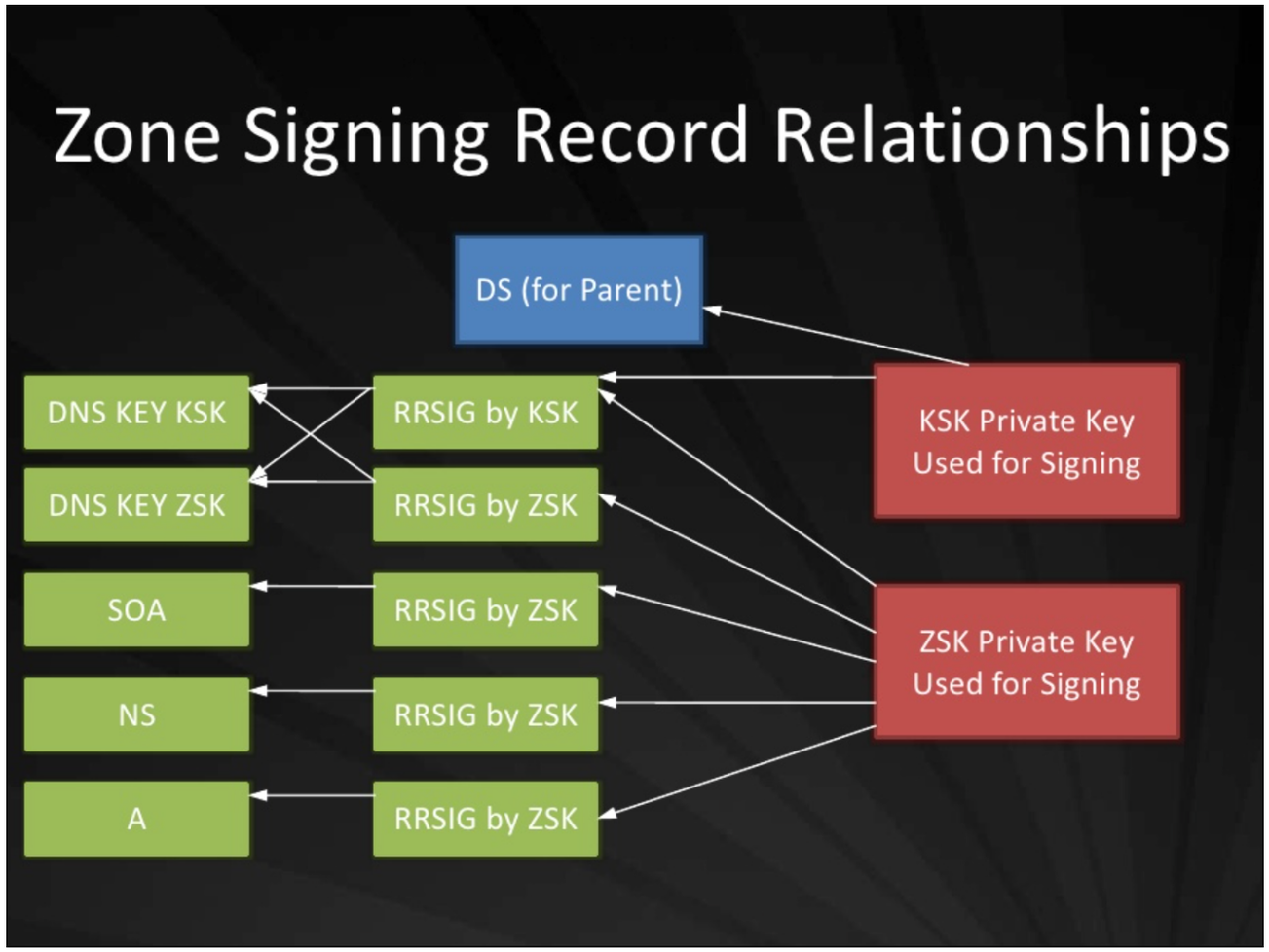
- 2 Key Pairs Used
  - ZSK (Zone Signing Key)
  - KSK (Key Signing Key)

ZSK

- Signs the Zone Records, and Itself
- Public Part Becomes the DNSKEY

KSK

- Signs the Keys at the Zone
- Public Part also becomes a DNSKEY



Stolen From Online…

Rollover

- RRSIGS Have lifetime they are valid for encoded in them
- DNSKEYs also have lifetime encoded in
  - Per NIST SP800-01
    - KSK — 12 Months (1 year)
    - ZSK — 30 Days (1 Month)
  - Both Current and future keys can put published at same time to support this

NIST SP800-01: National Institute of Standards and Technology (part of Dept of Commerce) Security and Privacy Controls for Federal Information Systems and Organizations

Resolvers

- Trust Anchors
- Validation

Trust Anchors

- Records used to validate RRSIGS for DNSKEY
- Many Forms:
  - Manually Obtained
  - DS Records at parent
  - DNS Lookaside
  - Root Signed SEP

secure entry point (Now that root is signed, these are less of issue)

Validation

- DNS Query with DNSSEC enabled
- Along with Response, RRSIG is returned
- Use DNSKEY from Zone (public part of ZSK) to validate the RRSIG
- Validate that DNSKEY with RRSIG
- Validate RRSIG with Public Key from KSK (trust anchor)
- If No Trust Anchor, go upwards for DS , validate. Lather, Rinse, Repeat

Implementation

- Authoritative (NSD)
- Recursive / Caching (unbound)

Authoritative

- Assume that NSD is already installed / configured to serve Authoritative Answers
- We will be signing example.com

Generate Keys

- cd /usr/local/etc/nsd/zones
- export ZSK=`ldns-keygen -a RSASHA1-NSEC3-SHA1 -b 1024 example.com`
- export KSK=`ldns-keygen -k -a RSASHA1-NSEC3-SHA1 -b 2048 example.com`

- 2 private keys with .private extension
- 2 public keys with .key extension
- 2 DS records with .ds extension

Sign The Zone

- ldns-signzone -n -s $(head -n100 /dev/random | sha1 | cut -b 1-16) example.com $ZSK $KSK
- tell NSD to use the signed zone (edit config file and point zonefile to example.com.zone.signed)

Generate DS Keys

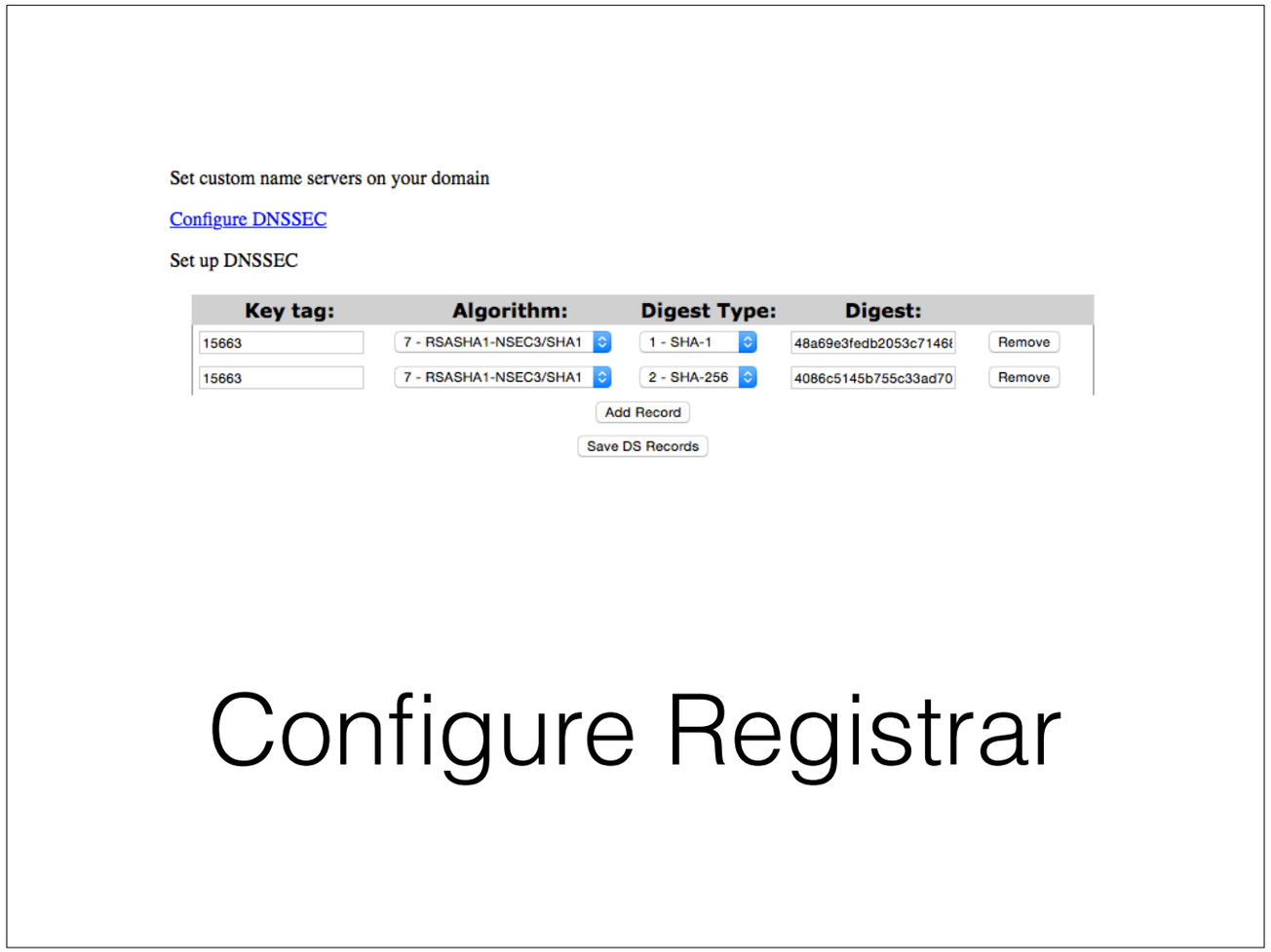
- rm $ZSK.ds $KSK.ds
- ldns-key2ds -n -1 example.com.zone.signed
- ldns-key2dn -n -2 example.com.zone.signed

We need these in a different format so remove them.

-n writes to standard out as opposed to file.
-1 will generate SHA1, -2 generates SHA256

```
0 example.com. 1800    IN      DS      17385 7 1 c1b9f7f1425bc44976dc19165e48c60032e7820d
1 example.com. 1800    IN      DS      17385 7 2 98216f4d66d24dbb752c46523a747a97bbad49d5846bbaa6256b6950b4a40995
```

Domain, TTL , IN , TYPE (DS), Keytag, Algorithm, Digest Type, Digest



Configure Registrar

Before you try to do this make sure your registrar supports this, if not find a new one :)

Verify Operation

- http://dnssec-debugger.verisignlabs.com/
- http://dnsviz.net/

VERISIGN // LABS

Domain Name: labratsoftware.com

Analyzing DNSSEC problems for labratsoftware.com

.	Found 2 DNSKEY records for . DS=19036/SHA-1 verifies DNSKEY=19036/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=19036 and DNSKEY=19036/SEP verifies the DNSKEY RRset
com	Found 1 DS records for com in the . zone Found 1 RRSIGs over DS RRset RRSIG=1518 and DNSKEY=1518 verifies the DS RRset Found 2 DNSKEY records for com DS=30909/SHA-256 verifies DNSKEY=30909/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=30909 and DNSKEY=30909/SEP verifies the DNSKEY RRset
labratsoftware.com	Found 2 DS records for labratsoftware.com in the com zone Found 1 RRSIGs over DS RRset RRSIG=35864 and DNSKEY=35864 verifies the DS RRset Found 2 DNSKEY records for labratsoftware.com DS=15663/SHA-256 verifies DNSKEY=15663/SEP Found 1 RRSIGs over DNSKEY RRset RRSIG=15663 and DNSKEY=15663/SEP verifies the DNSKEY RRset labratsoftware.com A RR has value 64.22.33.83 Found 1 RRSIGs over A RRset RRSIG=45632 and DNSKEY=45632 verifies the A RRset

Move your mouse over any ⊗ or ⚠ symbols for remediation hints.

Want a second opinion? Test labratsoftware.com at dnsviz.net.

Making Changes

- editing .signed file directly will invalidate zone
- Edit unsigned Zone (making sure to increment SOA Serial) and then resign the zone file

[No Name] + - VIM

```
#!/bin/bash
ZONEDIR="/usr/local/etc/nsd/zones" #location of your zone files
DOMAIN=$1
cd $ZONEDIR
KSK=$(basename $(grep -r "`grep '(ksk)' $DOMAIN.zone.signed | cut -f3-10`" K$DOMAIN.*.key | cut -d':' -f1) .key)
ZSK=$(basename $(grep -r "`grep '(zsk)' $DOMAIN.zone.signed | cut -f3-10`" K$DOMAIN.*.key | cut -d':' -f1) .key)
/usr/local/bin/ldns-signzone -n -p -s $(head -n 1000 /dev/random | sha1 | cut -b 1-16) -f $ZONEDIR/$DOMAIN.zone.signed $DOMAIN.zone $ZSK $KSK
/usr/local/sbin/nsd-control reload $DOMAIN
/usr/local/sbin/nsd-control notify $DOMAIN
```

zonesigner

Rollover

- Need to resign the zones every 30 days
- If you are making changes all the time, this isn't a problem, but if your zones are static, you need to make sure to do it ever 20 or so days (to account for propagation / caching). update the SOA and resign

Recursive/Caching

- Unbound has built in support
- auto-trust-anchor-file / unbound-anchor tool
- https://data.iana.org/root-anchors/root-anchors.xml

base Install supports it , as does ports on freebsd
unbound-anchor uses the IANA cert to verify the root anchor if it changed while system was off, else it will use RFC5011 probes to keep it updated during operation