DNSSEC...

... is the juice still worth the squeeze?!

Security

Benefits and Justification

About me...

- Author:
  - RFC7344 - "Automating DNSSEC Delegation Trust Maintenance"
  - RFC7646 - "Definition and Use of DNSSEC Negative Trust Anchors"
  - RFC8145 - "Signaling Trust Anchor Knowledge in DNS Security Extensions (DNSSEC)"
  - RFC8198 - "Aggressive Use of DNSSEC-Validated Cache"
  - RFC8509 - "A Root Key Trust Anchor Sentinel for DNSSEC"

About me...

- Author (cont.):
  - RFC8767 - "Serving Stale Data to Improve DNS Resiliency"
  - RFC8806 - "Running a Root Server Local to a Resolver"
- Formed and ran the IETF DNS-based Authentication of Named Entities (DANE) WG to replace CAs with DNSSEC
- ICANN SSAC member, contributing to multiple DNSSEC related advisories
- Consultant to USC/ISI, helping run b.root-servers.net

Security vs Stability

Issues and Concerns

What does DNSSEC provide?

3. Services Provided by DNS Security

The Domain Name System (DNS) security extensions provide origin authentication and integrity assurance services for DNS data, including mechanisms for authenticated denial of existence of DNS data.

What does DNSSEC provide?

- Cache poisoning protection
  - Off-path is largely solved, and on-path is a DoS
- Origin authentication
- Integrity assurance
- Authenticated denial of existence (NSEC)

What do users want?

They **don't** care about:

- cache poisoning
- origin authentication
- integrity assurance
- authenticated denial of existence...

They **do** care about:

- when the page says www.bigbank.com, it **is** BigBank
- when they send mail to their uncle, it reaches their uncle

What users want

DNSSEC doesn't actually accomplish their goal...

It authenticates that the address received for www.bigbank.com is the address that the zone operator intended.

- This, of course, assumes validation.
  - No-one **actually** validates; they just trust a bit that says that their resolver did...

What users want

TLS provides this...

- Yes, certs can be mis-issued
  - I, too, remember DigiNotar
  - Certificate Transparency helps
- Yes, users can bypass the big scary warning
- Yes, not everything is signed yet...
  - See RFC6797 - "HTTP Strict Transport Security (HSTS)"
  - 132,000+ sites already preloaded

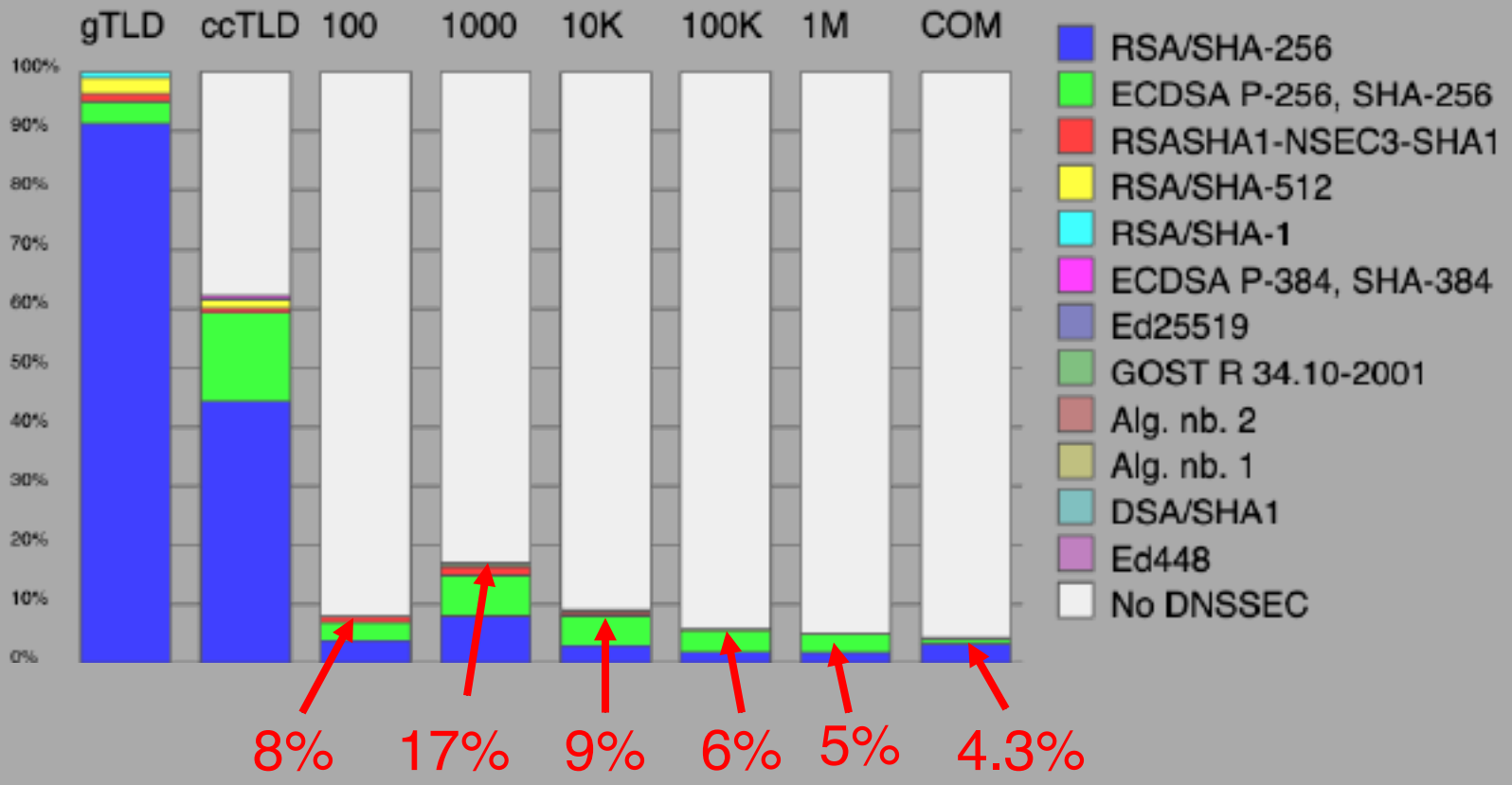
- Yes, not everything is the web. But for most users, it is.

State of deployment

- RFC4033 published in 2005 (18 years ago)
- Root Zone was signed in 2010 (13 years ago)
- All gTLDs signed
- Most ccTLDs signed

So, mission accomplished?

State of deployment



Src: https://ithi.research.icann.org/graph-m11.html#M11Top

But everyone validates, right? *Right?!*

Code	Region	DNSSEC Validates	Partial Validates
XA	World	30.48%	8.49%
XF	Oceania	42.93%	3.11%
XE	Europe	39.04%	9.49%
XC	Americas	33.02%	7.04%
XB	Africa	29.88%	13.86%
XD	Asia	27.46%	7.77%

69% don't...

57% don't...

61% don't...

67% don't...

70% don't...

72% don't...

Oh, and 100% of stubs don't

Src: https://stats.labs.apnic.net/dnssec

Yeah, so what?

- If DNSSEC were free, this would be fine
- People could use it if they want, and ignore it they don't
  - Sadly, DNSSEC doesn't work like that

DNSSEC failures affect the domain, **and everyone under it**

But failures are rare, right? *Right?!*

Notable TLD failures...

- .tn — Tunisia (May 2021)
- .xn--y9a3aq — Armenia (July 2021)
- .bn — Brunei (July 2021)
- .xn--qxam — Greek IDN (August 2021)
- .tm — Turkmenistan (December 2021)
- .se — Sweden (February 2022) partial
- .fj — Fiji (March 2022)
- .au — Australia (March 2022)
- .ma — Morocco (April 2022) partial
- .bn — Brunei (May 2022)

Src: https://ianix.com/pub/dnssec-outages.html

Notable TLD failures (cont.)...

- .kg — Kyrgyzstan (August 2022)
- .kg — Kyrgyzstan (August 2022)
- .tm — Turkmenistan (September 2022)
- .na — Namibia (October 2022)
- .xn--qxam — Greek IDN (November 2022)
- .mx — Mexico (April 2023)
- .nz — New Zealand (May 2023)
- .ve — Venezuela (July 2023)
- *.au — Australia (September 2023)

Src: https://ianix.com/pub/dnssec-outages.html

Lusser's law...

$$R_s = \prod_{i=1}^{N} r_i = r_1 \times r_2 \times r_3 \times \ldots \times r_n$$

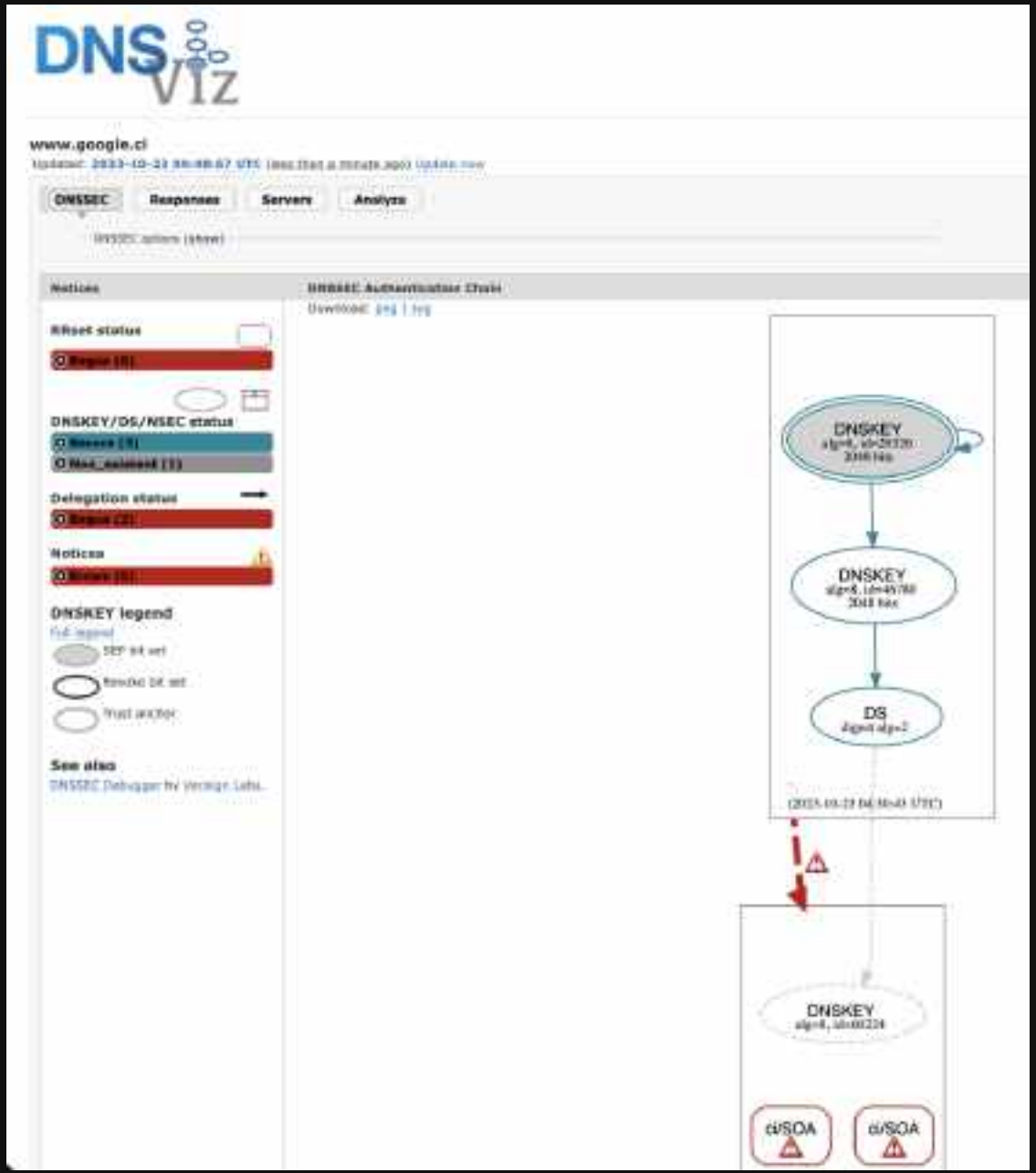
Rs is the overall reliability of the system, and *rn* is the reliability of the *n*th component.

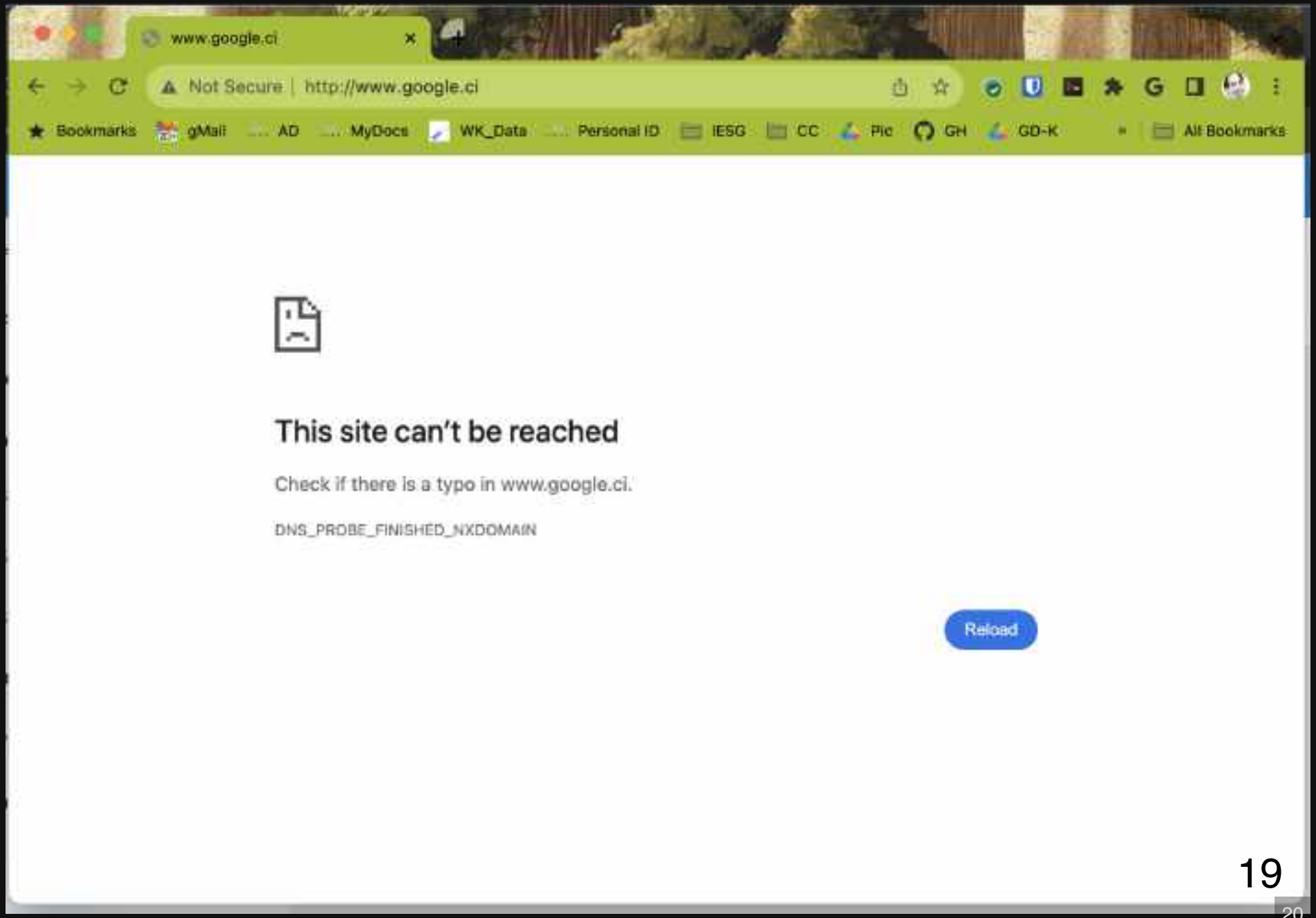
The reliability of a system is bounded by that of the weakest dependency.

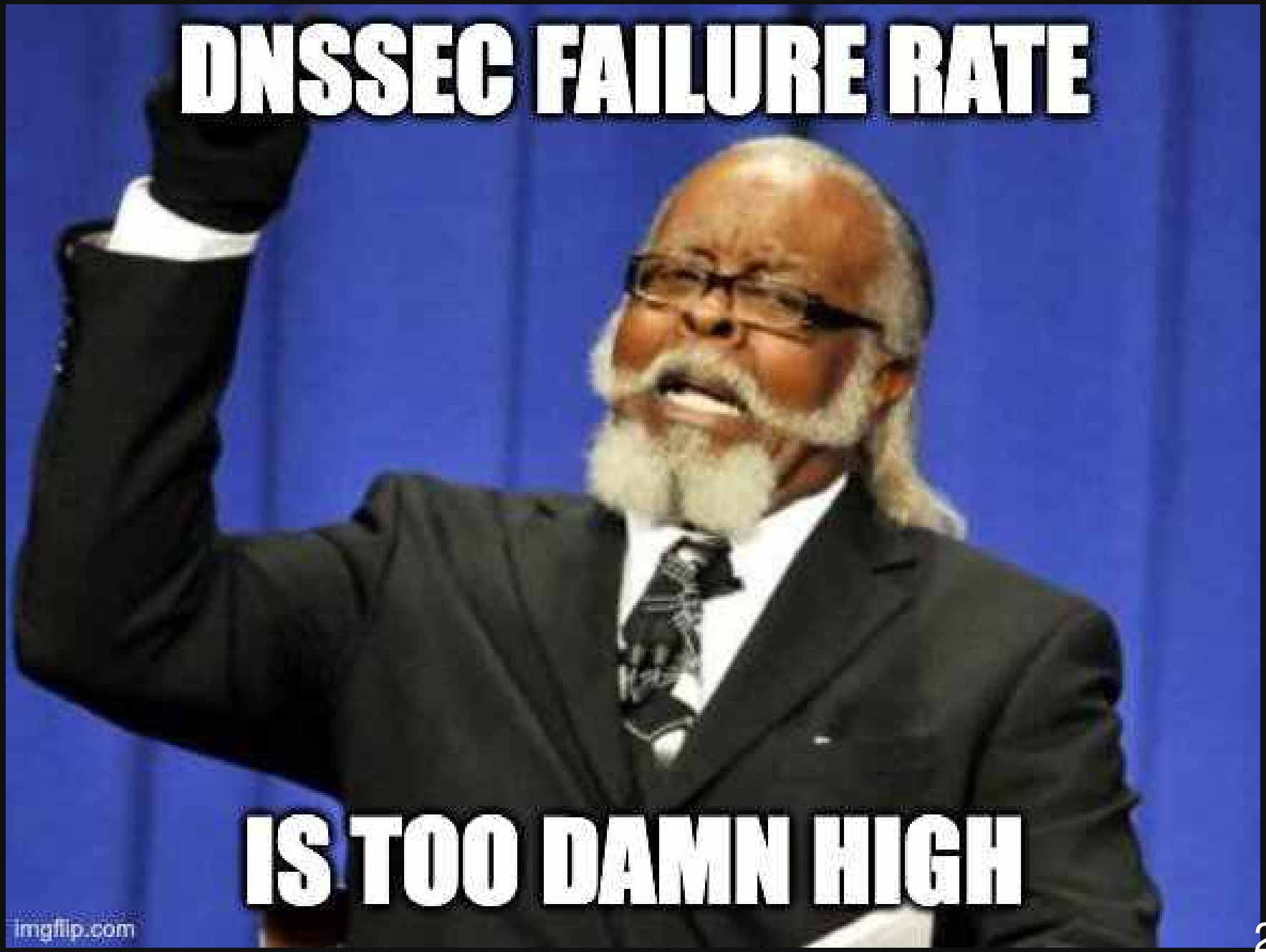
"You cannot build a system with nine nines with a dependency on a four nines component..."

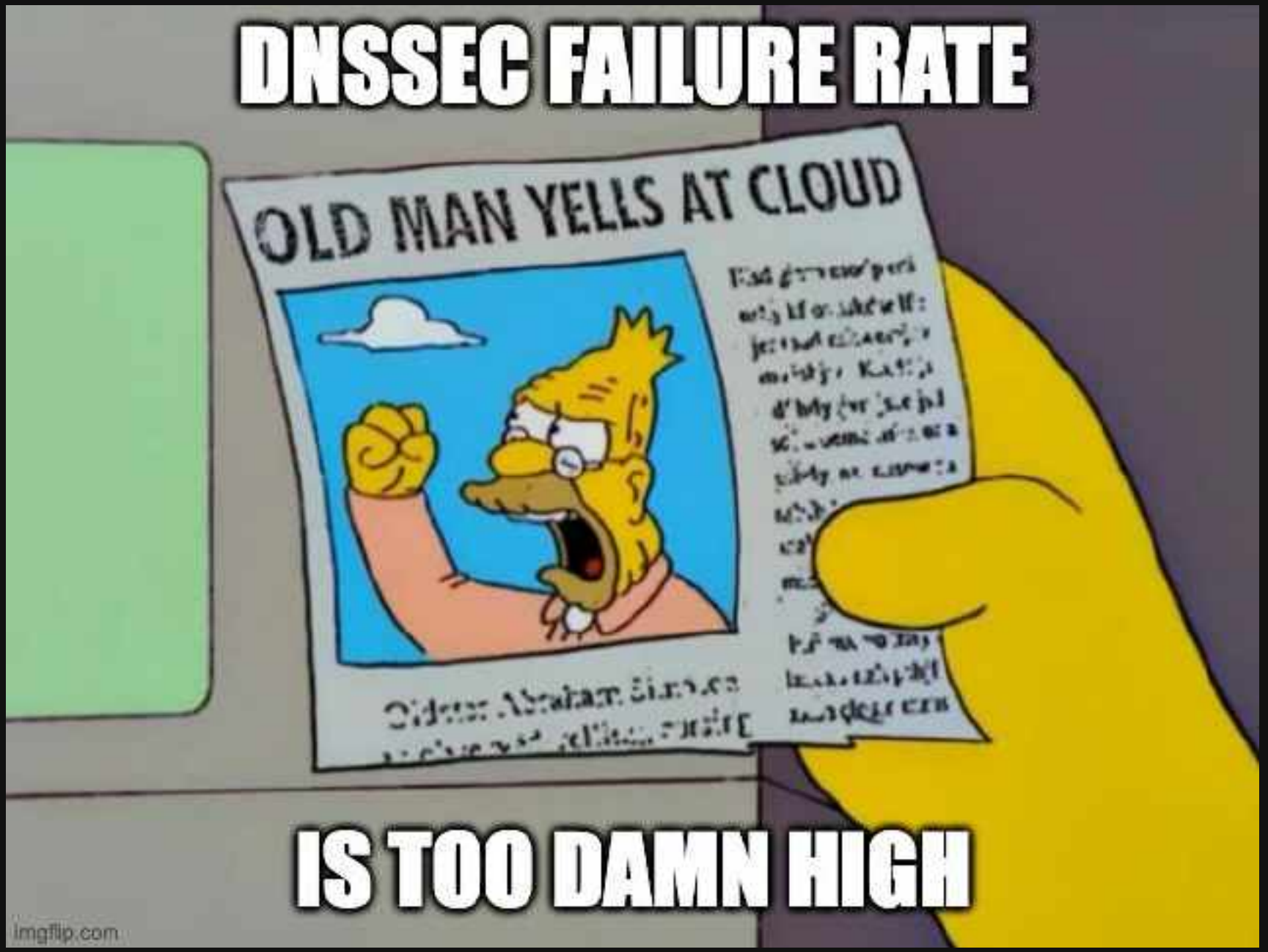
17

No matter how reliable you make your service, it still breaks if your parent screws up their DNSSEC...


DNSViz
www.google.ci
DNSSEC
Responses
Servers
Analysis
Notices
DNSSEC Authentication Chain
RRset status
DNSKEY/DS/NSEC status
Delegation status
Notices
DNSKEY legend
See also
DNSKEY
DNSKEY
DS
DNSKEY
d/SOA
d/SOA


www.google.ci
Not Secure | http://www.google.ci
Bookmarks
gMail
AD
MyDocs
WK_Data
Personal ID
IESG
CC
Pic
GH
GD-K
All Bookmarks
This site can't be reached
Check if there is a typo in www.google.ci.
DNS_PROBE_FINISHED_NXDOMAIN
Reload


DNSSEC FAILURE RATE
IS TOO DAMN HIGH
imgflip.com


DNSSEC FAILURE RATE
OLD MAN YELLS AT CLOUD
IS TOO DAMN HIGH
imgflip.com

So, what's my point?

- No, I don't think we should deprecate DNSSEC
  - It's really useful for infrastructure
  - People who want it should be able to use it
    - My personal domains are all signed
    - ZONEMD is great!
    - Whee, Aggressive NSEC!
    - Yay for DANE for SMTP!

Again, what's the point?

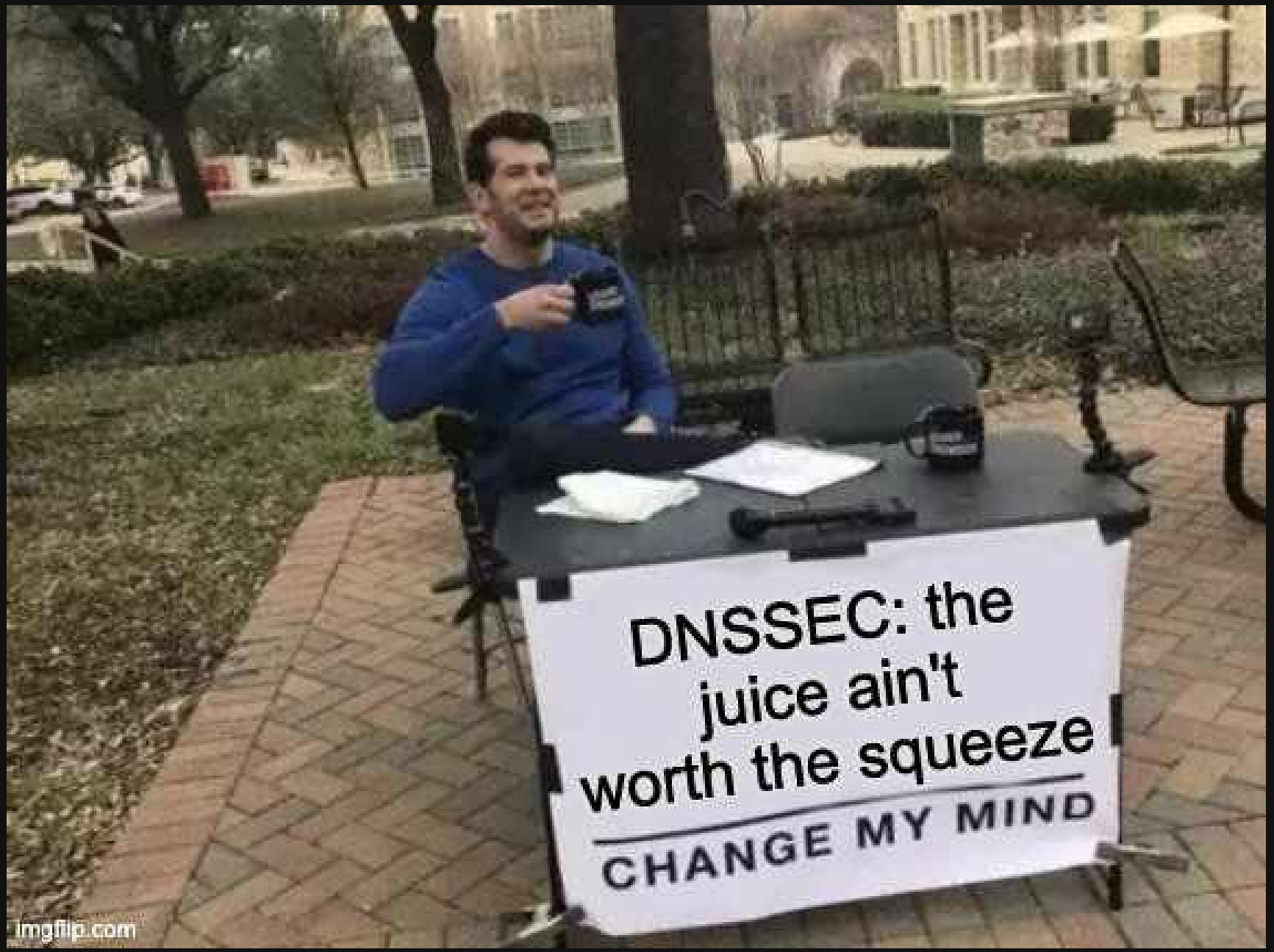
- The system needs to be **much much** more reliable
  - Until it is, we should stop evangelizing DNSSEC

"Just DNSSEC Harder!!!!" is not the answer.

"If we just do X, we can fix it..." is also not the answer.

We need to take a deep look at the reliability issues, and figure out how to make the whole system less fragile.

Until then, promoting DNSSEC does more harm than good.


DNSSEC: the juice ain't worth the squeeze
CHANGE MY MIND
imgflip.com

Backup Slides

Major site failures...

- cdc.gov (January 2021)
- dnscrypt.pl (February 2021)
- dnssek.info (March 2021)
- parler.com (April 2021)
- epa.gov (April 2021)
- nih.gov (April 2021)
- nist.gov (June 2021)
- lequipe.fr (June 2021)
- slack.com (September 2021)

Src: https://ianix.com/pub/dnssec-outages.html

Major site failures...

- europa.eu (December 2021)
- dnsops.gov (February 2022)
- europa.eu (March 2022)
- gsu.edu (March 2022)
- temple.edu (May 2022)
- nist.gov (June 2022)
- nohats.ca (July 2022)
- dnssec-name-and-shame.com (July 2022)

Src: https://ianix.com/pub/dnssec-outages.html

Major site failures...

- mail.mil (September 2022)
- ns{1..4}.dnsimple.com (September 2022) Broken black lies implementation
- mail.mil (November 2022)
- 41.in-addr.arpa/NS (December 2022)
- tamu.edu (January 2023)

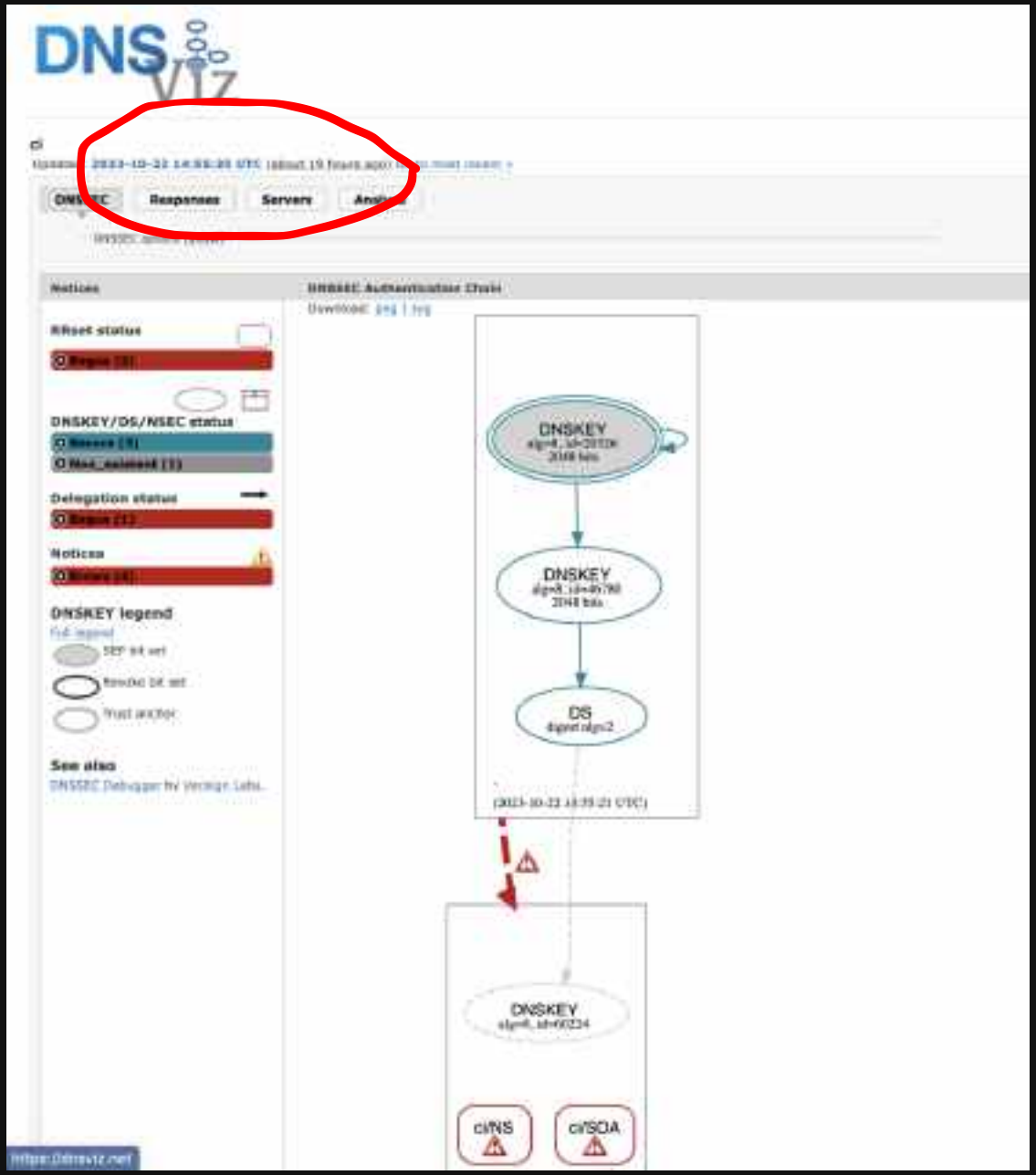
I believe that the admin of this list has largely given up at this point.

Src: https://ianix.com/pub/dnssec-outages.html

Links and similar:

- "Calling time on DNSSEC: The costs exceed the benefits"
  -- Matt Brown
- "Operational Experience with DNSSEC Signed Zones"
  -- Shumon Huque
- "DNSSEC – The Journey at a Crossroads"
  -- Ed Lewis

31


DNS
Responses
Servers
Notices
DNSKEY/DS/NSEC status
Delegation status
Notices
DNSKEY legend
See also
DNSKEY
DNSKEY
DS
DNSKEY
cNS
cSOA


google.ci
Safari Can't Find the Server
Safari can't open the page "www.google.ci" because Safari can't find the server "www.google.ci".