DELEG: DNS op de schop

Delegeren als een pro! Veilig en met vertrouwen.

Willem Toorop
willem@nlnetlabs.nl

– 15 april 2025 –

DELEG?

- “DNSSEC - The Journey at a Crossroads”
  Ed Lewis, Video vanaf 33:40
  ICANN DNS Symposium (september 2023)

Internet **C**orporation for **A**ssigned **N**ames and **N**umbers
beheerder van namen en nummers op het internet

- Does Not Scale: Rethinking DNS for the Future of the Internet
  Hackathon project tijdens IETF 118 (november 2023)
  20 deelnemers - Resultaat: draft-wesplaap-deleg

Internet **E**ngineering **T**ask **F**orce
een standaarden organisatie voor protocollen op het internet

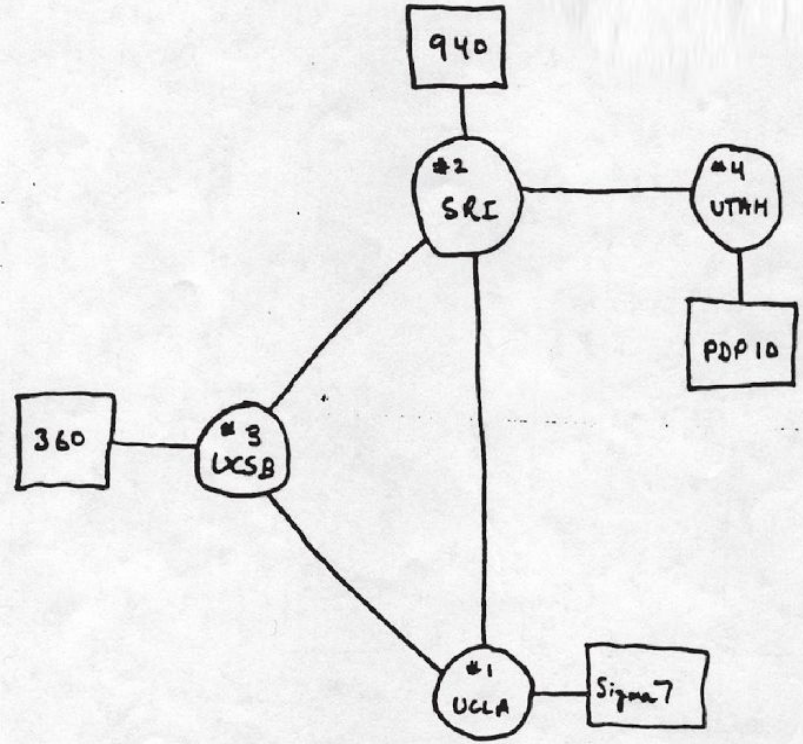
DELEG?

- juni 2024 : DNS Delegation (deleg) werkgroep opgericht
- juli 2024 : Tweede protocol draft-homburg-deleg
- oktober 2024 : Document van vereisten gepubliceerd
- maart 2025 : IETF 122 in Bangkok
  : Start selectie tussen wesplaap en homburg
- 8 april 2025 : Stoppen met stemmen
- 14 april 2025 : wesplaap-deleg is gekozen

In deze presentatie

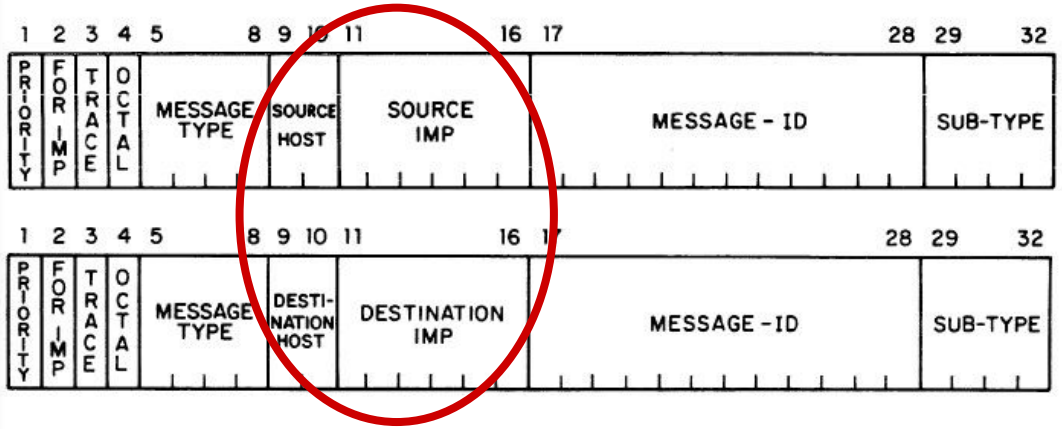
- Ontstaan van DNS (9 slides: 5-13)
  - met delegaties als het centrale idee
- Delegaties in de DNS op dit moment (15 slides: 12-26)
- Tekortkomingen van delegaties in de DNS (5 slides: 22-26)
  - Niet veilig
  - Niet privé
  - Moderne operationele praktijk slecht vertegenwoordigd
- Hoe DELEG dit allemaal adresseert (14 slides: 19-42)

Ontstaan van DNS



THE ARPA NETWORK

DEC 1969



- Network Control Protocol
- Interface Message Processors
- Max 64 IMPs met max 4 hosts = maximum van 256 hosts

Ontstaan van DNS

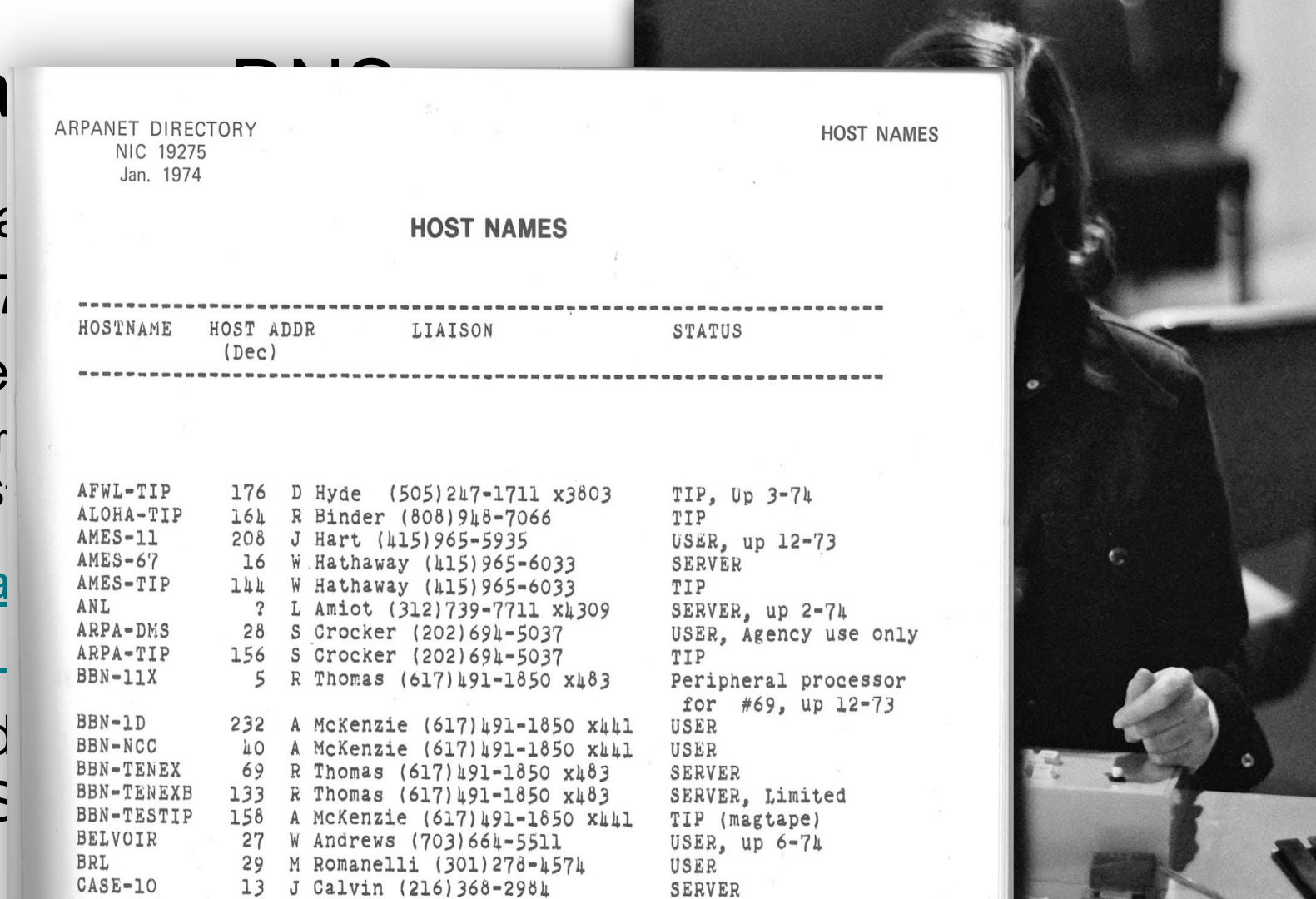
- Centraal beheerde Hosts table van 1971 tot 1987 beheer door Elizabeth “Jake” Feinler

  van het Arpanet Network Information Center (NIC) at Stanford Research Institute (SRI)

- “Host Tables, Top-Level Domain Names, and the Origin of Dot Com”
- Vanaf december 1973 HOSTS.TXT (RFC 606)

Ontstaa

- Centraa
  van 197
  Elizabe
  van het Ar
  (NIC) at S
- “Host Ta
  Names,
- Vanaf d
  HOSTS



ARPANET DIRECTORY
NIC 19275
Jan. 1974

HOST NAMES

HOSTNAME	HOST ADDR (Dec)	LIAISON	STATUS
AFWL-TIP	176	D Hyde (505)247-1711 x3803	TIP, Up 3-74
ALOHA-TIP	164	R Binder (808)948-7066	TIP
AMES-11	208	J Hart (415)965-5935	USER, up 12-73
AMES-67	16	W Hathaway (415)965-6033	SERVER
AMES-TIP	144	W Hathaway (415)965-6033	TIP
ANL	?	L Amiot (312)739-7711 x4309	SERVER, up 2-74
ARPA-DMS	28	S Crocker (202)694-5037	USER, Agency use only
ARPA-TIP	156	S Crocker (202)694-5037	TIP
BBN-11X	5	R Thomas (617)491-1850 x483	Peripheral processor for #69, up 12-73
BBN-1D	232	A McKenzie (617)491-1850 x441	USER
BBN-NCC	40	A McKenzie (617)491-1850 x441	USER
BBN-TENEX	69	R Thomas (617)491-1850 x483	SERVER
BBN-TENEXB	133	R Thomas (617)491-1850 x483	SERVER, Limited
BBN-TESTIP	158	A McKenzie (617)491-1850 x441	TIP (magtape)
BELVOIR	27	W Andrews (703)664-5511	USER, up 6-74
BRL	29	M Romanelli (301)278-4574	USER
CASE-10	13	J Calvin (216)368-2984	SERVER

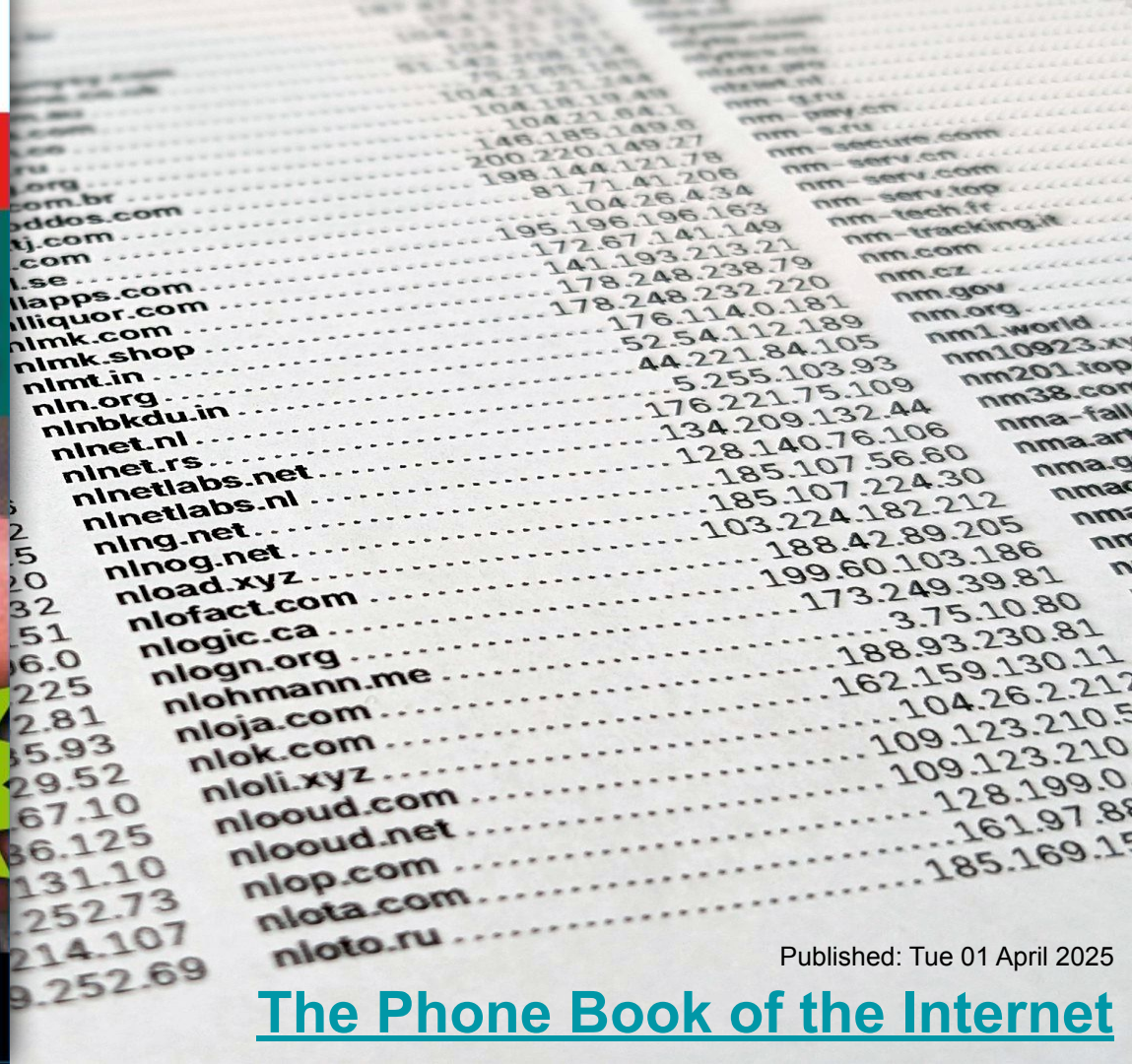
University of Twente
The Netherlands

NetLabs

2025 Edition

the Internet

"Hands down best use of OpenINTEL I have ever seen!" -Roland van Rijswijk-Deij



Published: Tue 01 April 2025

The Phone Book of the Internet

Ontstaan van DNS

- Vint Cerf werkte van ‘73 tot ‘79 aan de opvolger van NCP: Transmission Control Protocol

IEN 151

Vint Cerf
DARPA/IPTO
1 April 80

FINAL REPORT OF THE STANFORD

UNIVERSITY TCP PROJECT

Vinton G. Cerf
1 April 1980

ABSTRACT:

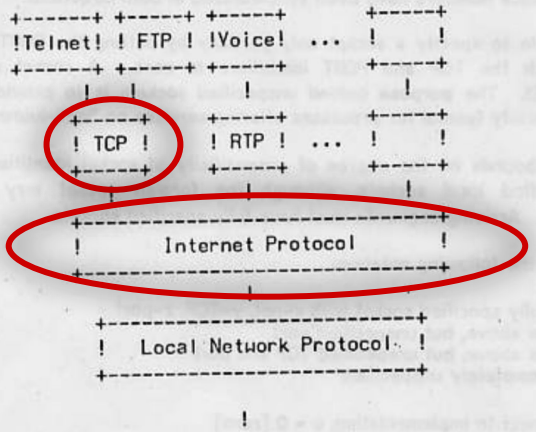
This report provides a brief historical and technical summary of the Stanford University internet, host-to-host Transmission Control Protocol (TCP) project. Developed from 1973-1976 at Stanford, Bolt Beranek and Newman and University College London, the effort then continued at other research and development centers during 1977-1980. Originally designed as a monolithic internet protocol, the internet aspects were separated into a distinct protocol layer in early 1979 with the publication of version 4 of TCP. The resulting pair of protocols, TCP4 and Internet Protocol (IP) are now undergoing procedures for standardization within

Jon Postel

implemented without adverse effects, so this matching facility could be considered the minimum acceptable for TCP operation.

2.3. Functional Specification of Interfaces

The following diagram illustrates the place of the TCP in the protocol hierarchy:



Protocol Relationships

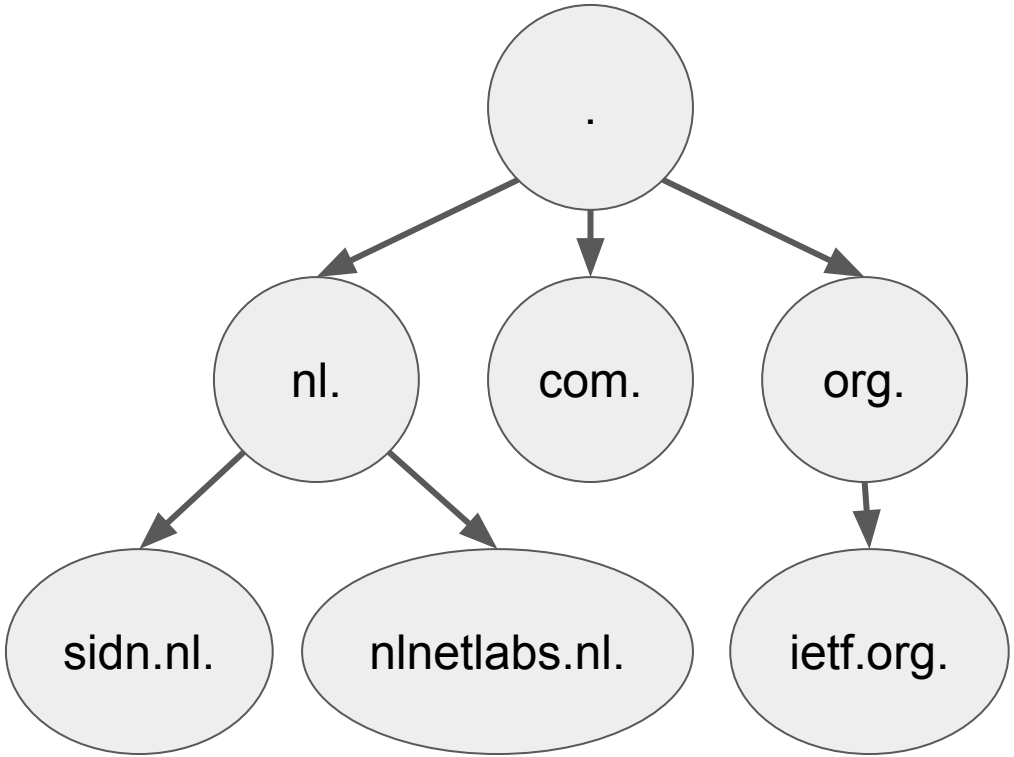
Figure 1.

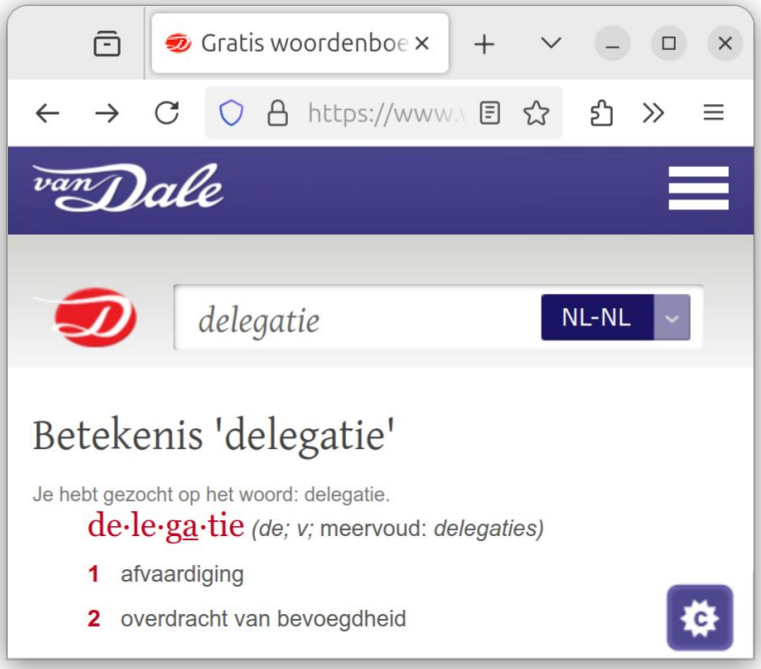
It is expected that the TCP will be able to support higher level protocols efficiently. It

Ontstaan van DNS

- 1 januari 1983: NCP → IP/TCP (*flag day)*
- max 256 → max 4.294.967.296 hosts
- **Een hosts tabel schaalt niet**
- november 1983: Paul Mockapetris: Domain Name System (RFC 882) Implementatie: JEEVES
- Since november 1987: STD 13

Domain Name System - Schaalbaar door delegaties



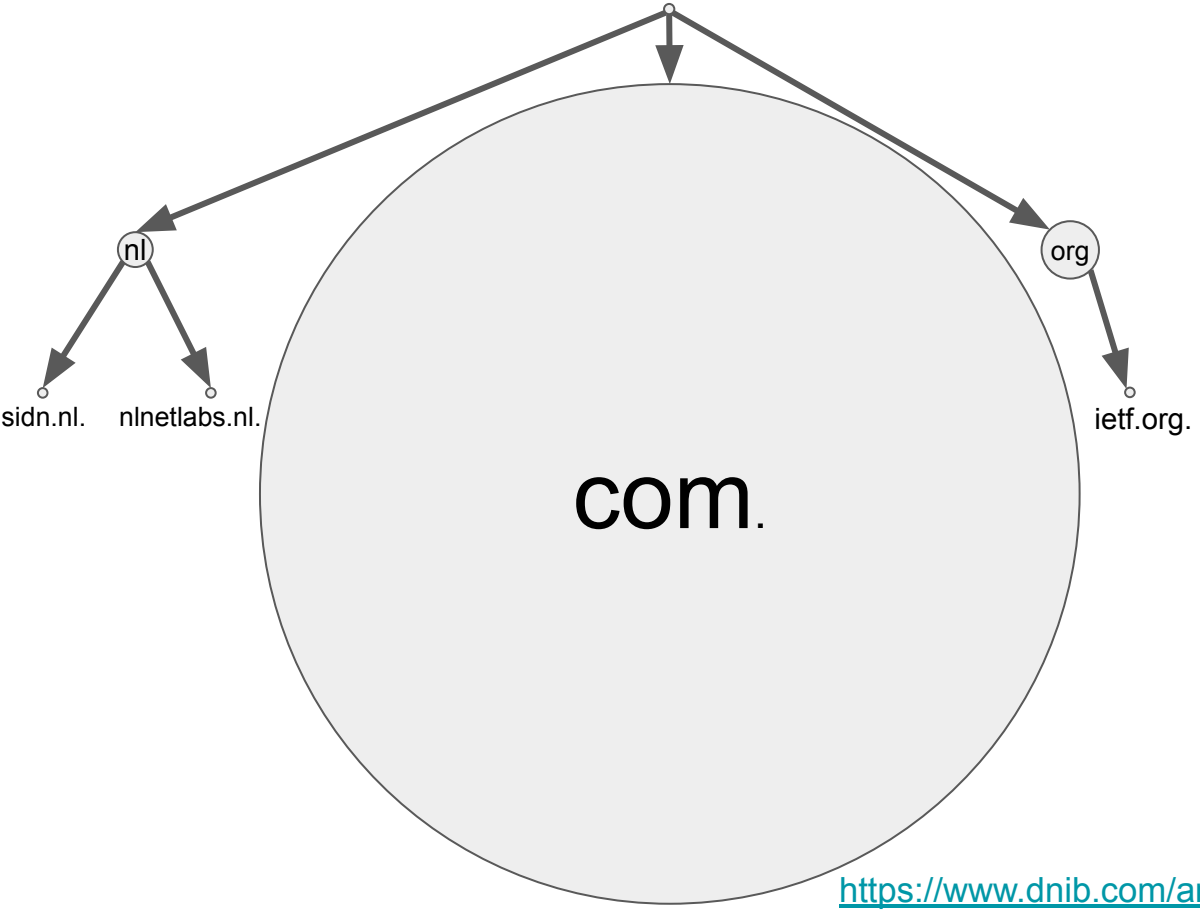


Transitie van HOSTS.TXT naar DNS (1982 – 1987)

- Jake Feinler bedenkt TLDs in 1982: .mil, .edu, .gov, .org, ~~.bus~~ and .com

- Namedroppers Working Group “to discuss naming”
- Incorporatie van: Defense Communications Agency (DCA) en Defense Advanced Research Projects Agency (DARPA) leidde tot de start van de Internet Engineering Task Force (IETF)[ref] in 1986

Domain Name System - Schaalbaar door delegaties

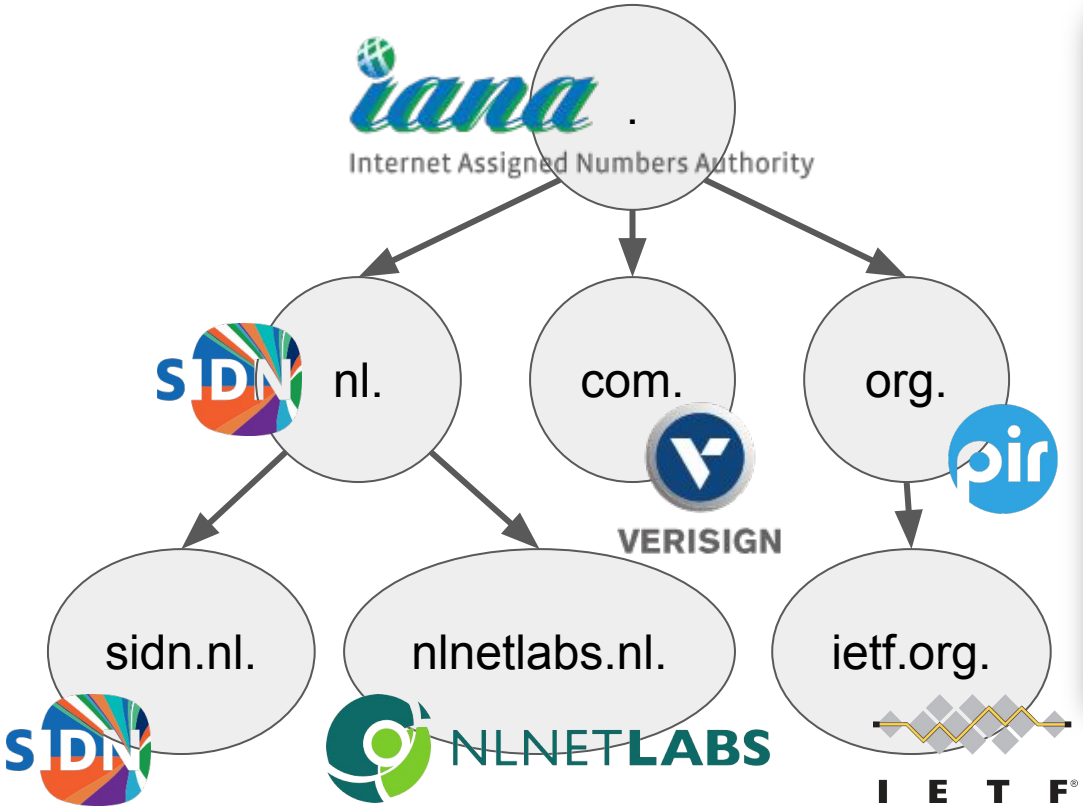


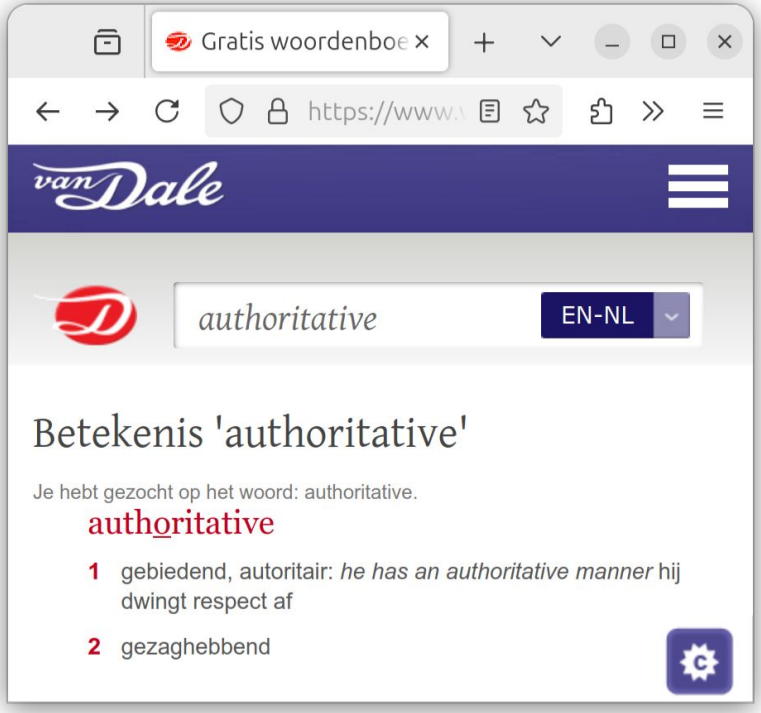
Niet helemaal gelijkmatig verdeeld

com.	156.3M
cn.	19.7M
de.	17.7M
net.	12.7M
org.	11.0M
uk.	10.3M
ru.	6.6M
nl.	6.2M
. (root)	1444
Totaal # registraties:	364.3M

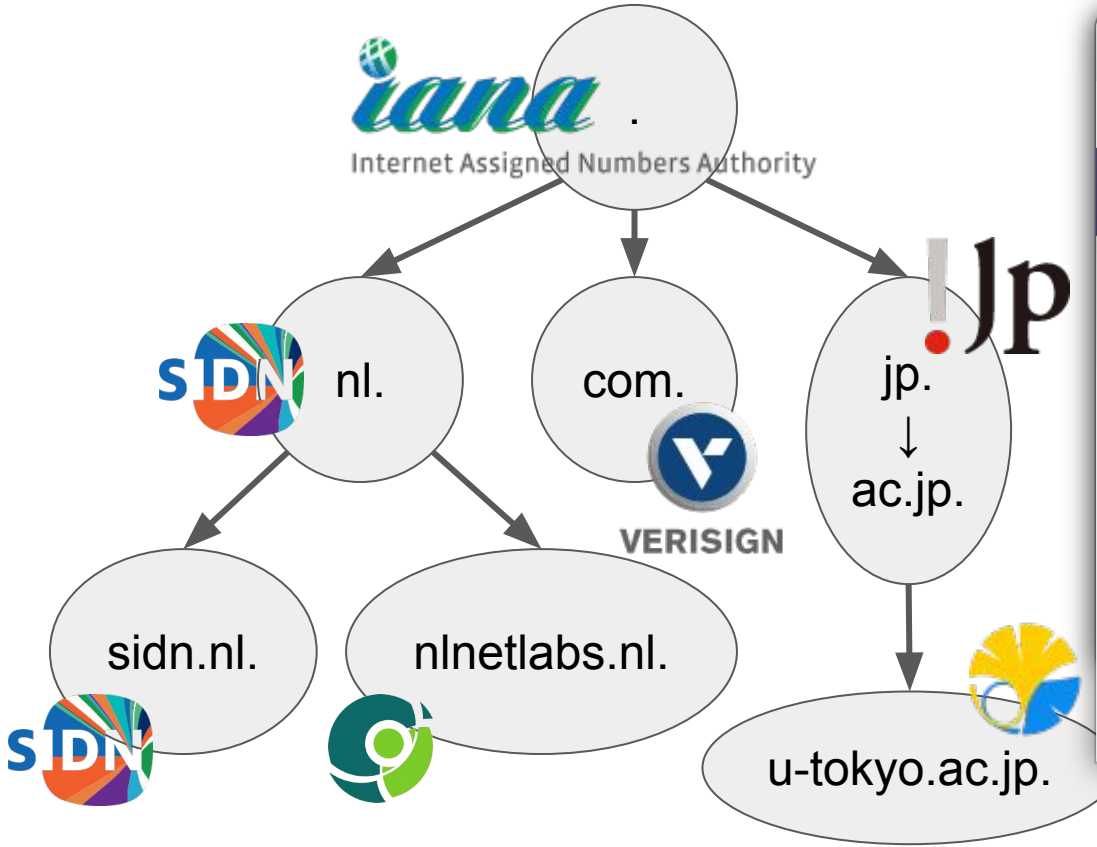
https://www.dnib.com/articles/the-domain-name-industry-brief-q4-2024

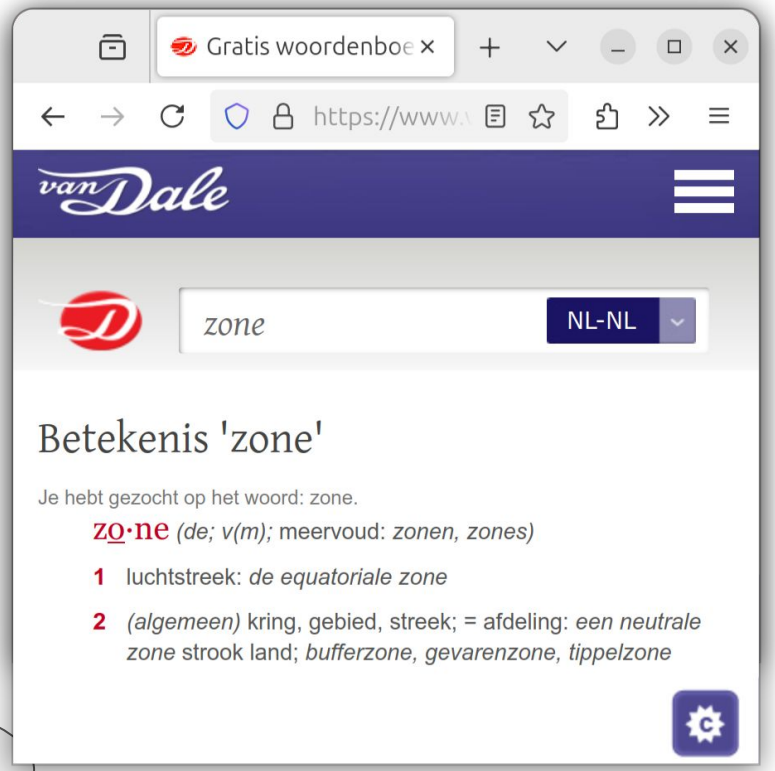
bevoegdheidsoverdracht aan de gezaghebbenden (autoritatief)



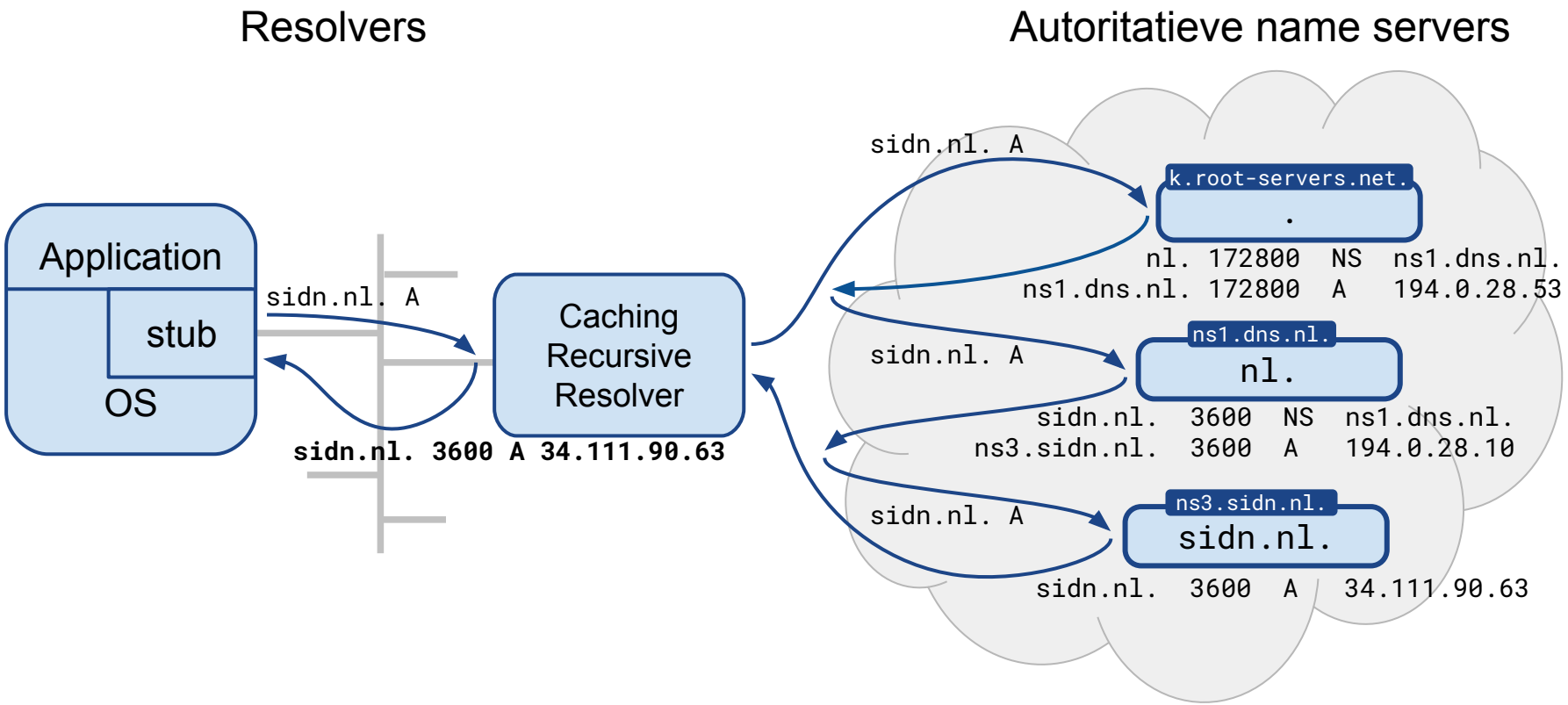


bevoegdheid over een gebied in de DNS (zone)

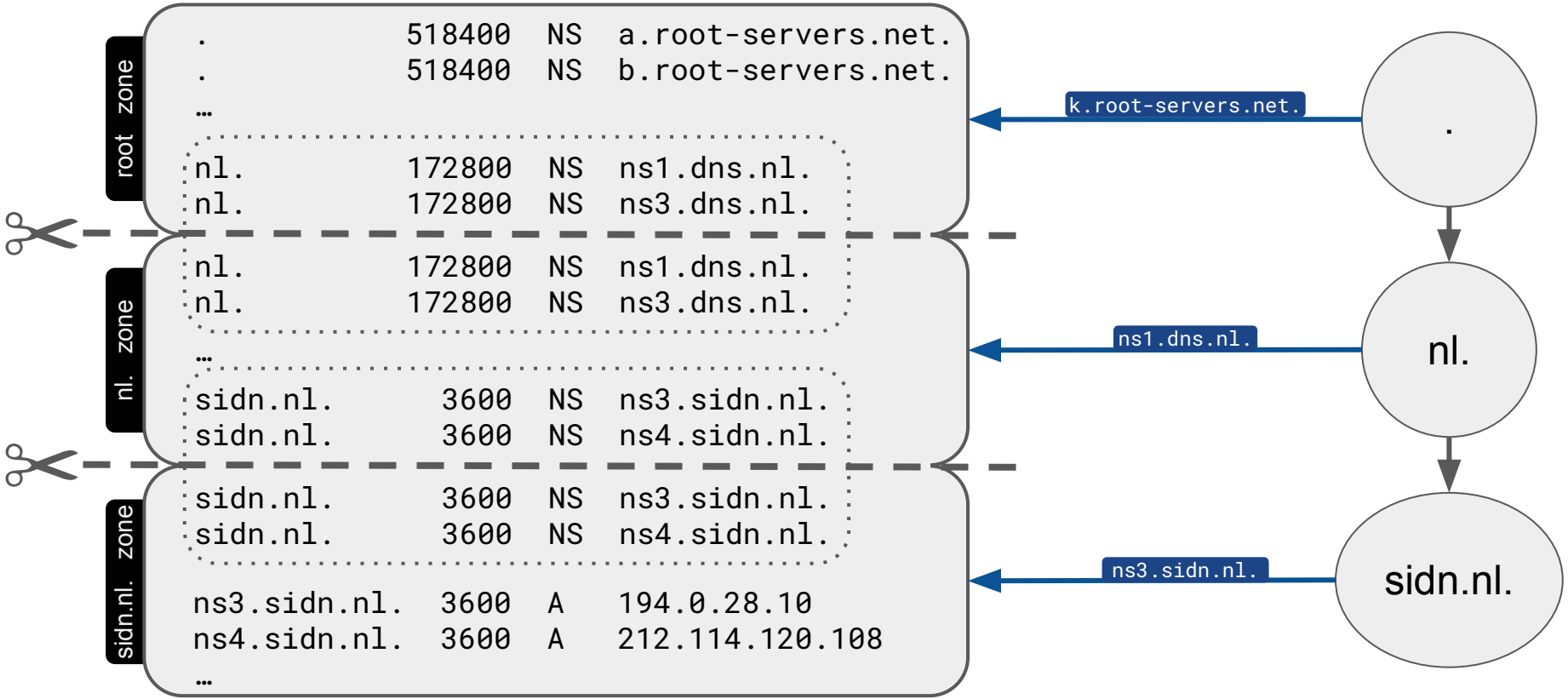




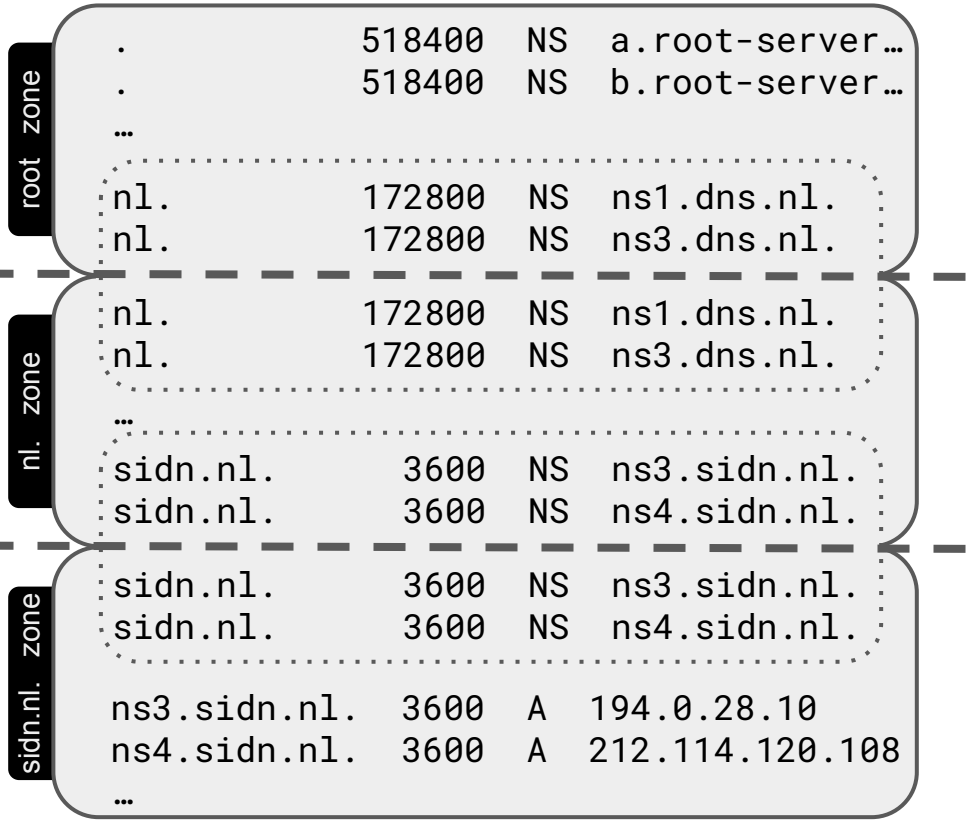
technisch gerealiseerd met name servers



Delegaties - de zone cut



Delegaties - de zone cut



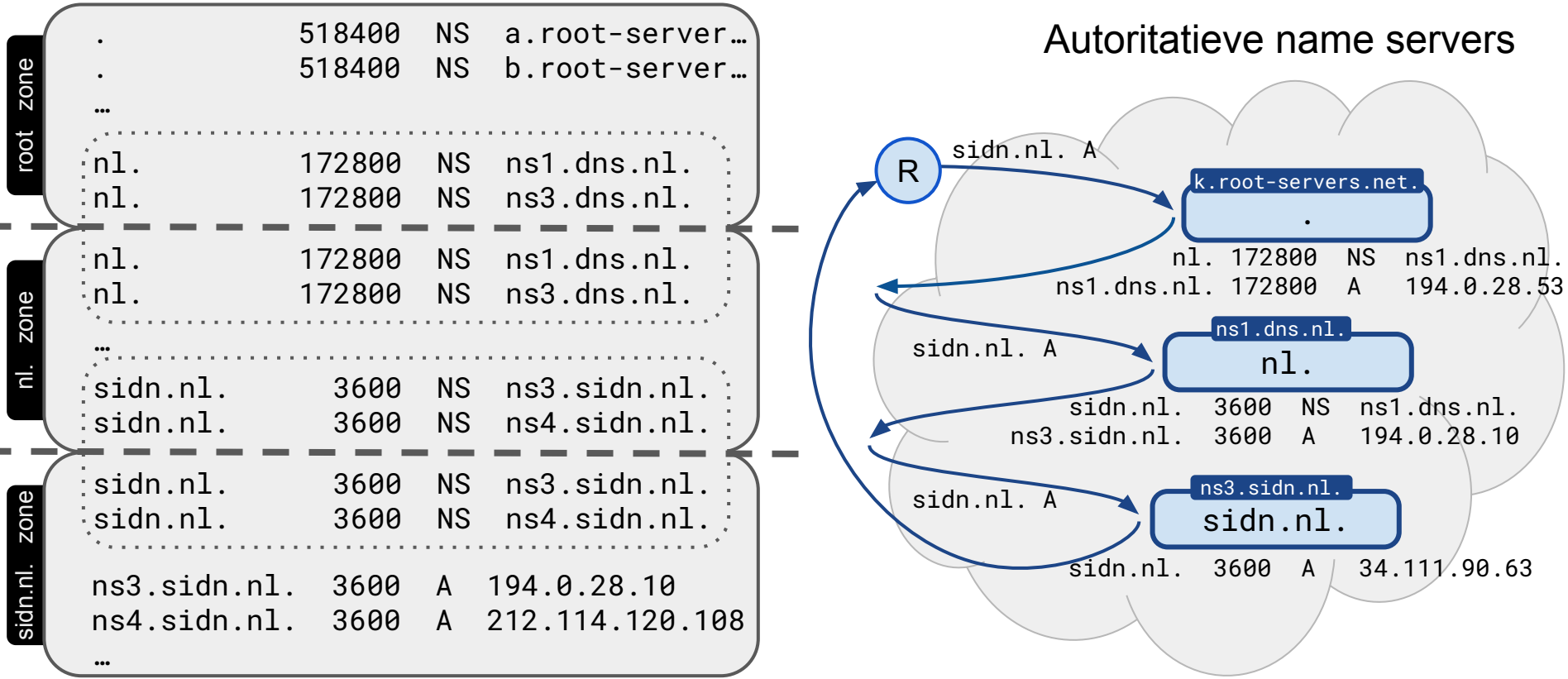
- *Boven* de zone cut aan de ouder zijde:

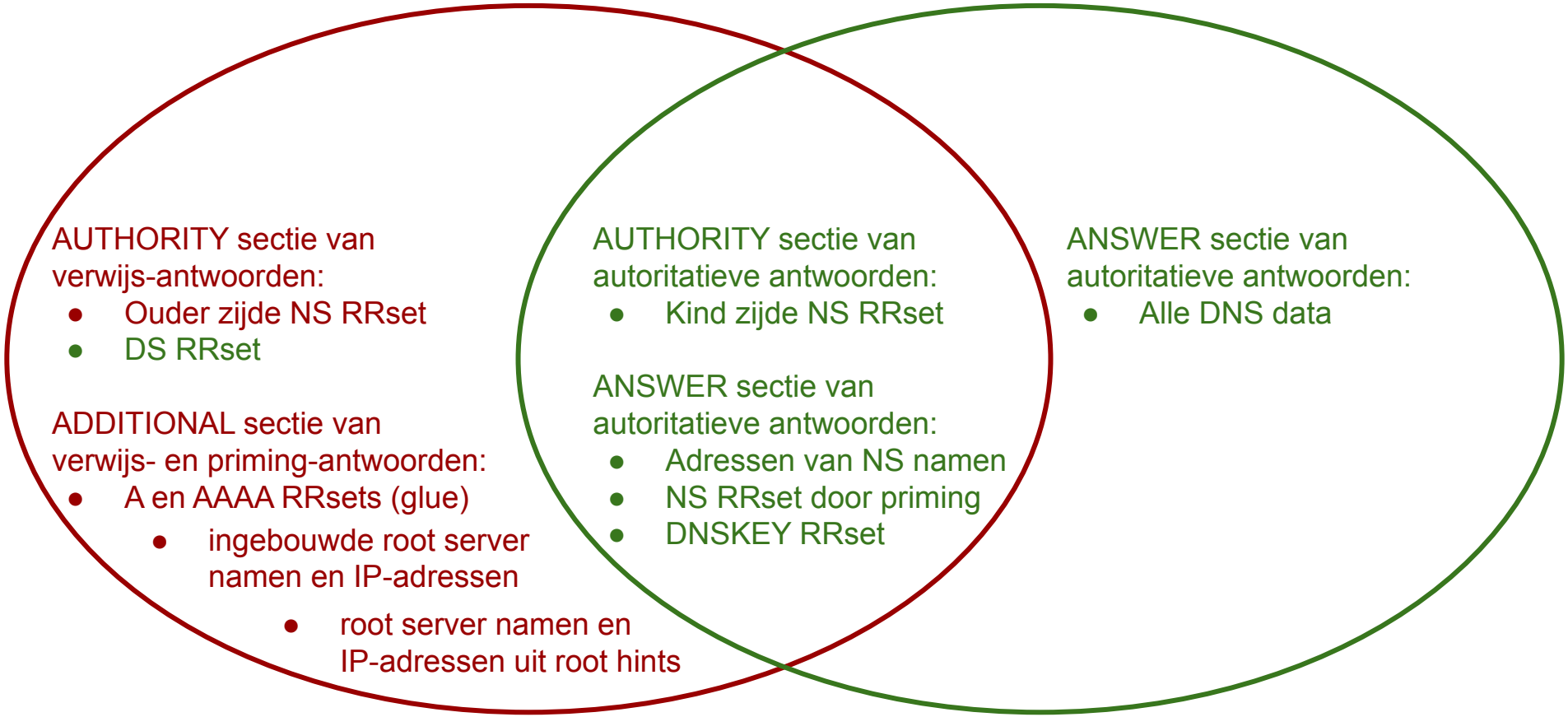
  Niet autoritatief

- *Onder* de zone cut aan de kind zijde:

  Autoritatief

Delegaties - de zone cut

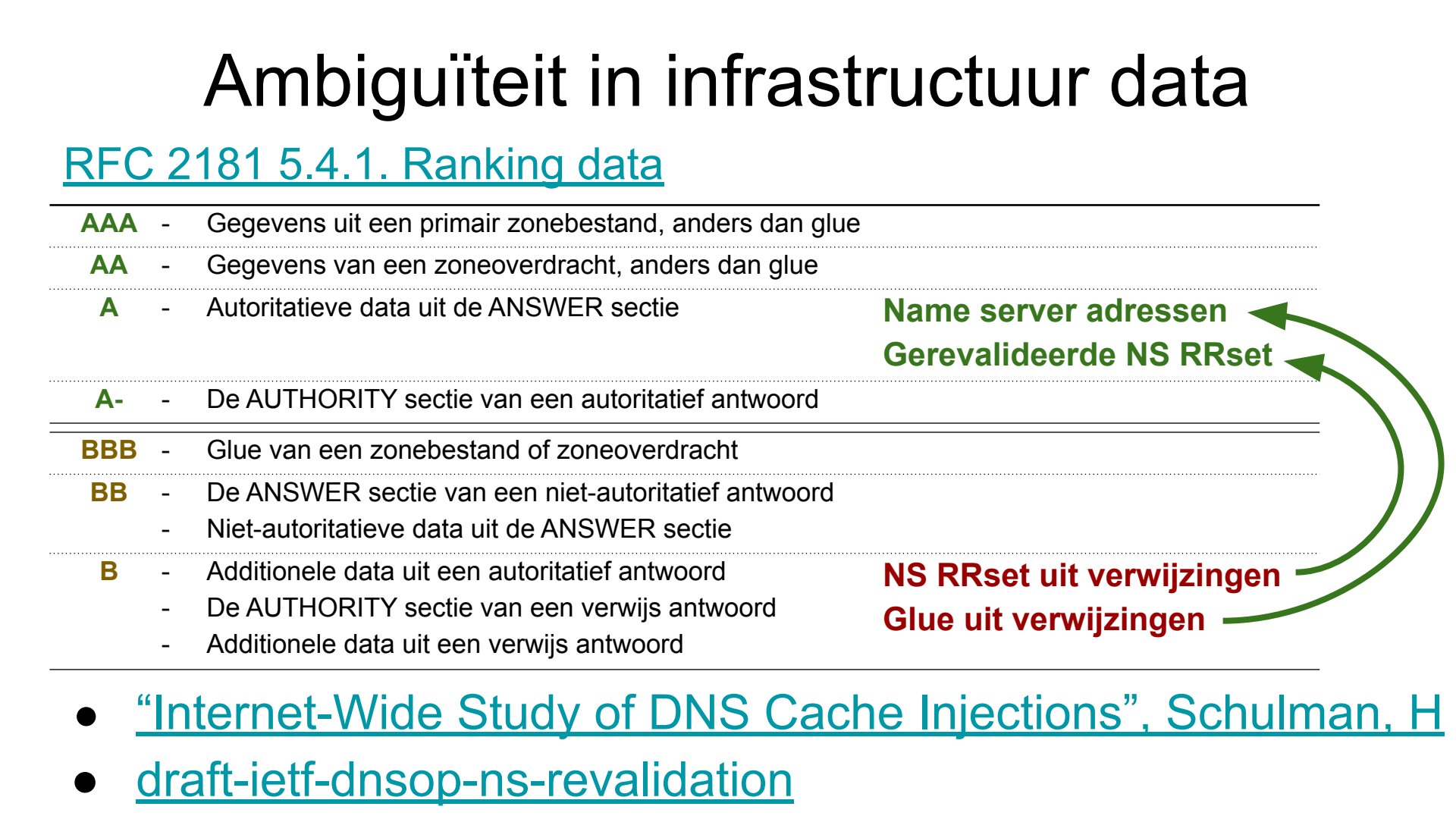



Infrastructuur data
gebruikt door resolvers
Autoritatieve data
geretourneerd door resolvers
AUTHORITY sectie van verwijs-antwoorden:
Ouder zijde NS RRset
DS RRset
ADDITIONAL sectie van verwijs- en priming-antwoorden:
A en AAAA RRsets (glue)
ingebouwde root server namen en IP-adressen
root server namen en IP-adressen uit root hints
AUTHORITY sectie van autoritatieve antwoorden:
Kind zijde NS RRset
ANSWER sectie van autoritatieve antwoorden:
Adressen van NS namen
NS RRset door priming
DNSKEY RRset
ANSWER sectie van autoritatieve antwoorden:
Alle DNS data

Ambiguïteit in infrastructuur data

RFC 2181 5.4.1. Ranking data

AAA	-	Gegevens uit een primair zonebestand, anders dan glue	
AA	-	Gegevens van een zoneoverdracht, anders dan glue	
A	-	Autoritatieve data uit de ANSWER sectie	**Name server adressen** **Gerevalideerde NS RRset**
A-	-	De AUTHORITY sectie van een autoritatief antwoord	
BBB	-	Glue van een zonebestand of zoneoverdracht	
BB	-	De ANSWER sectie van een niet-autoritatief antwoord	
	-	Niet-autoritatieve data uit de ANSWER sectie	
B	-	Additionele data uit een autoritatief antwoord	**NS RRset uit verwijzingen**
	-	De AUTHORITY sectie van een verwijs antwoord	**Glue uit verwijzingen**
	-	Additionele data uit een verwijs antwoord	



- "Internet-Wide Study of DNS Cache Injections", Schulman, H
- draft-ietf-dnsop-ns-revalidation

Ambiguïteit in infrastructuur data

RFC Ranking data

AA	rimair zonebestand, anders dan glue
A	zoneoverdracht, anders dan glue
	de ANSWER sectie
	van een autoritatief antwoord
	and of zoneoverdracht
	een niet-autoritatief antwoord
	it de ANSWER sectie
	utoritatief antwoord
	n een verwijs antwoord
	erwijs antwoord

Name server adressen

Gerevalideerde NS RRset

NS RRset uit verwijzingen

Glue uit verwijzingen

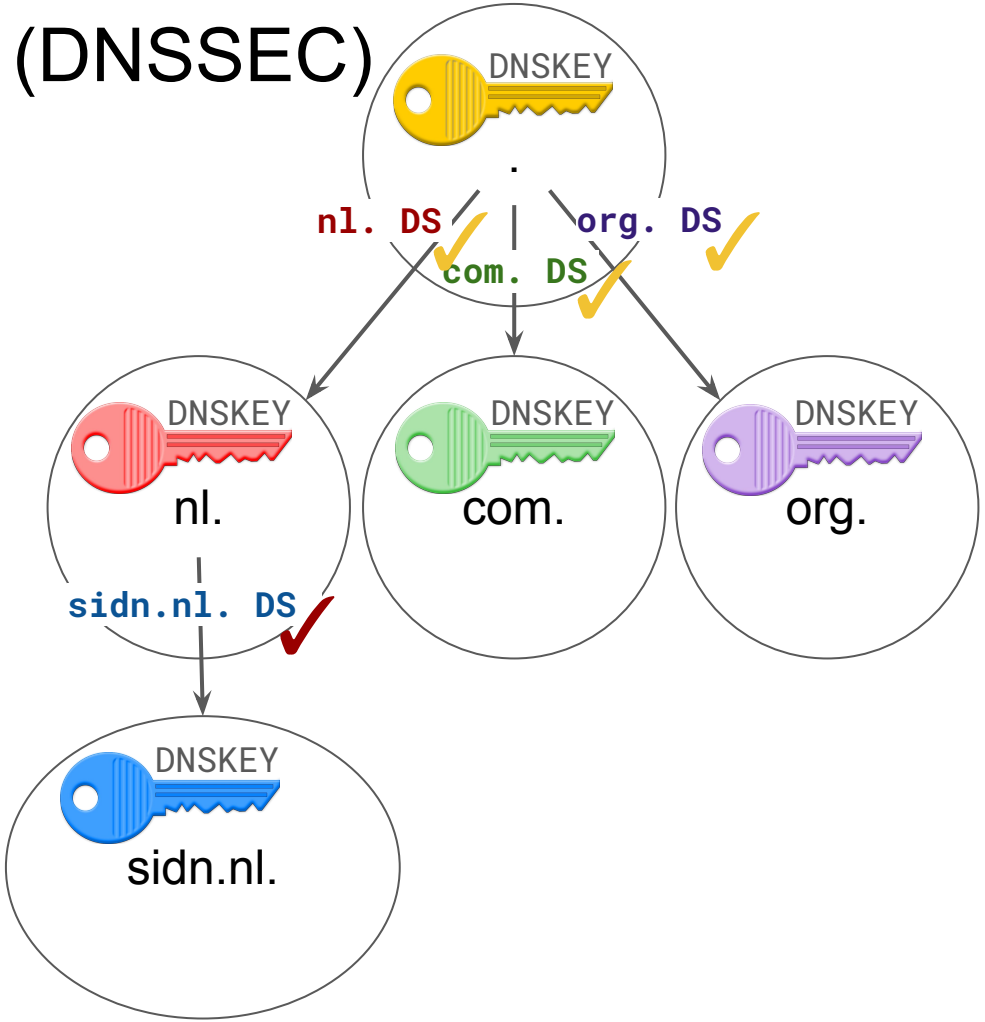
dy of DNS Cache Injections”, Schulman, H

revalidation

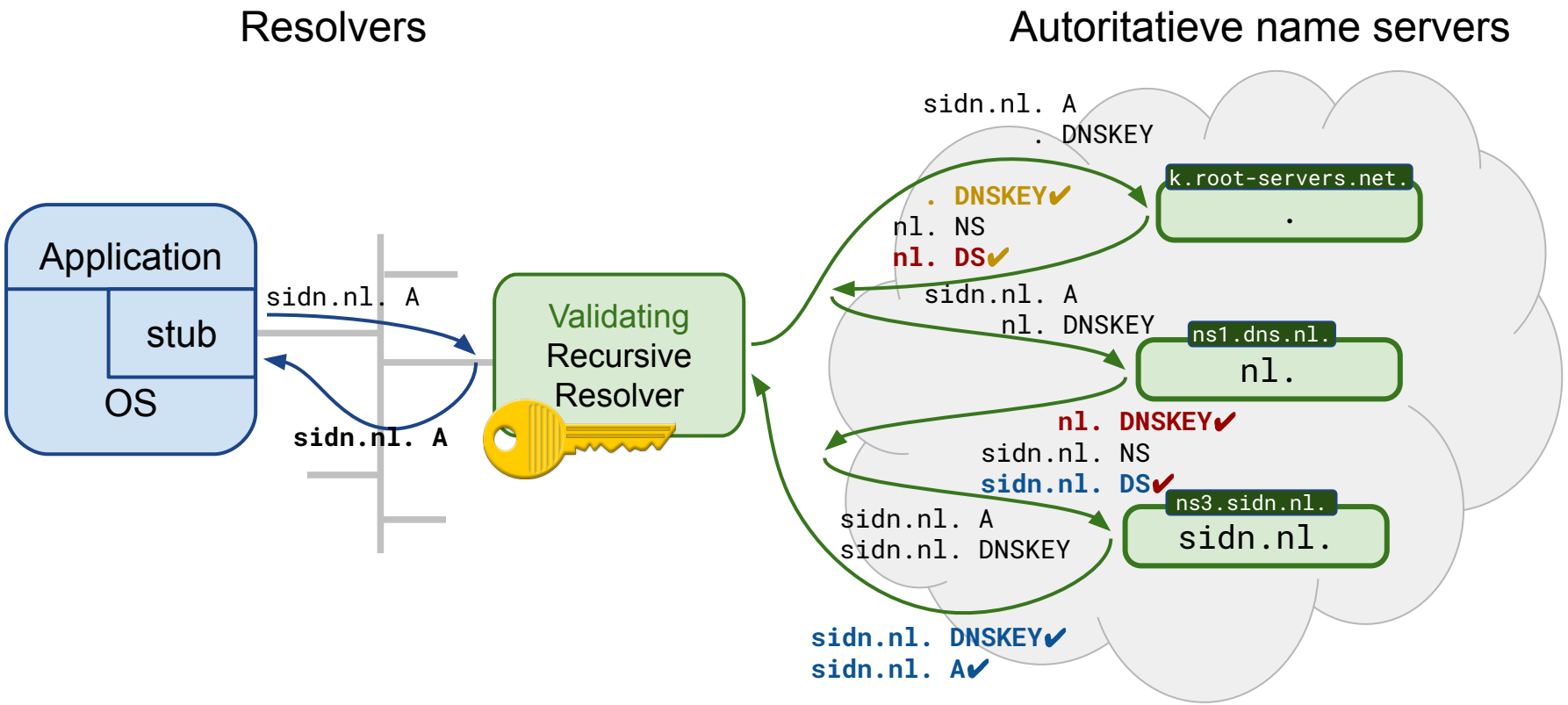
DNS Security Extensions (DNSSEC)

- DNSKEY : publieke sleutel van de zone
- DS : hash(DNSKEY) autoritatief aan de ouder zijde
- RRSIG : Signature

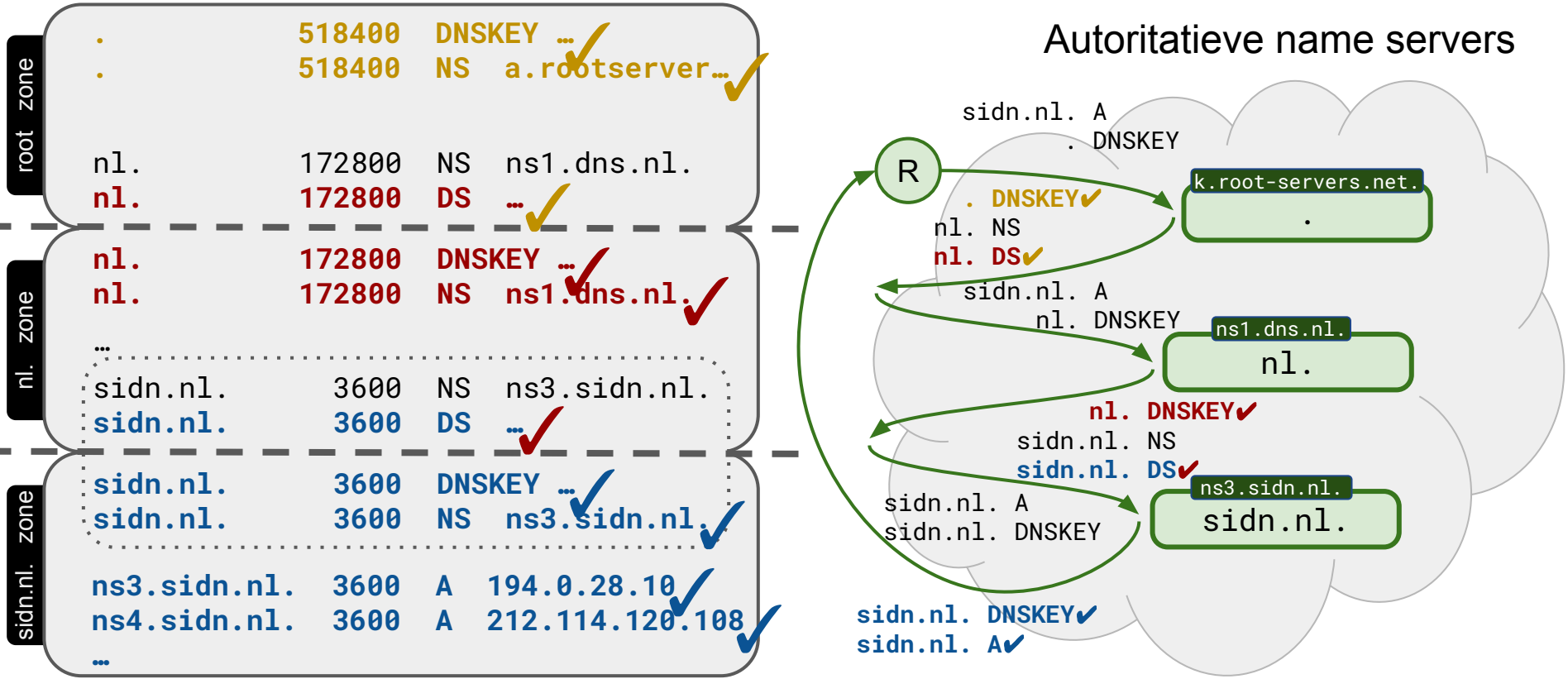
- “Chain of Trust” volgt de delegaties



De “Chain of Trust” volgt de delegaties



Maar de niet autoritatieve data is niet gesigned!



Maar de niet autoritatieve data is niet gesigned!

- Resolvers gebruiken de niet autoritatieve ouder zijde data
- Die niet gesigned is met DNSSEC
- Welke name server gecontact moet worden kan ongemerkt herschreven worden (omgeleid naar malafide name server)
- En vervolgens de delegaties in die zone omleiden, etc.

- Een privacy issue. De malafide name server ziet alle queries.
- Dit lijkt geen security zorg! (DNSSEC werkt, maar…)

ar de niet autoritatieve data is niet gesigned!

solvers gebruiken de niet

niet gesigned is met DN

e name server gec

Ben geen
DNSSEC snob
en help de unsigned!

The reduced risk of redirected query traffic with signed root name server data

“ Revalidation is the **only** mitigation that also works against **on-path** attackers!

DELEG harde vereisten — draft-ietf-deleg-requirements

H1. DELEG mag het bestaande registratiemodel voor domeinen niet verstoren

H2. DELEG moet backwards compatibel zijn

H3. DELEG mag geen negatieve impact hebben op de meeste DNS-software

H4. DELEG moet delegaties kunnen beveiligen met DNSSEC.

H5. DELEG moet updates van delegatie-informatie met hetzelfde relatieve gemak ondersteunen als momenteel

H6. DELEG moet stapsgewijs ingezet kunnen worden

H7. Meerdere onafhankelijke operators moeten een zone kunnen serven

H4. DELEG moet delegaties kunnen beveiligen met DNSSEC.

- Dus de delegatie informatie moet autoritatief zijn

In de delegerende (ouder) zone		*In de gedelegeerde (kind) zone*
Op de zone cut	*Elders autoritatief*	
• **`sidn.nl`** • wesplaap-deleg • pwouters-ds-uplifting • arends-parent-only-record-signalling	• **`sidn._deleg.nl`** • homburg-deleg	• **`_dns.ns3.sidn.nl`** • Vooral ideeën • dnsop-ns-revalidation vereist

Nog een uitzondering (zoals DS) of niet?

Op de zone cut (wesplaap-deleg)	*Elders autoritatief (homburg-deleg)*
`sidn.nl  DELEG  …`	**`sidn._deleg.nl  IDELEG  …`**
• Name servers, DNSSEC signers en validators en resolvers moeten allemaal aangepast worden.	• Werkt al met alleen resolver implementatie
• Nieuwe manier van doorverwijzen	• De oude vertrouwde manier van doorverwijzen (CNAME & DNAME)
• Alle name servers die een DELEG zone bedienen, moeten worden geüpgraded.	• Geen, gemengd of allemaal geüpgradede name servers werkt allemaal prima
• 0 extra queries	• Kan werken met 0 extra queries

DELEG zachte vereisten — draft-ietf-deleg-requirements

S1. DELEG moet nieuwe transportmechanismen mogelijk maken

S2. DELEG moet alle benodigde details voor de delegatie bevatten

S3. DELEG moet de benodigde transacties minimaliseren

S4. DELEG moet beheer van een DNS dienst versimpelen

S5. Conventionele DNS moet afgeleid kunnen worden van DELEG

S6. DELEG moet uitbreidbaar zijn met nieuwe functies

S7. DELEG moet een delegatie model sterker dan DNSSEC kunnen faciliteren

Privacy

maart 2011 : Privacy Considerations for Internet Protocols

juni 2013 : Snowden Revelations [Morecowbell]

juli 2013 : RFC 6973 Privacy Considerations for Internet Protocols

mei 2014 : RFC 7258 Pervasive Monitoring is an Attack

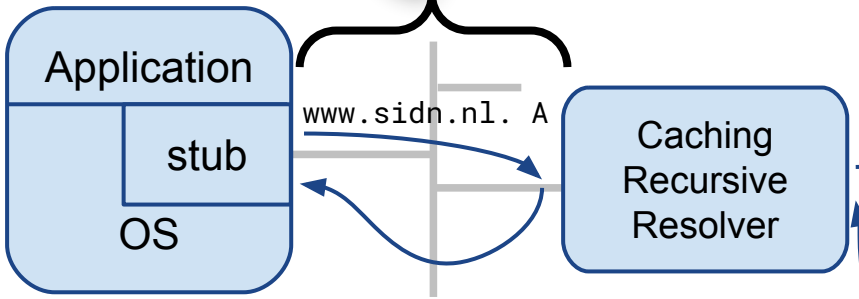
Overal
Encryptie

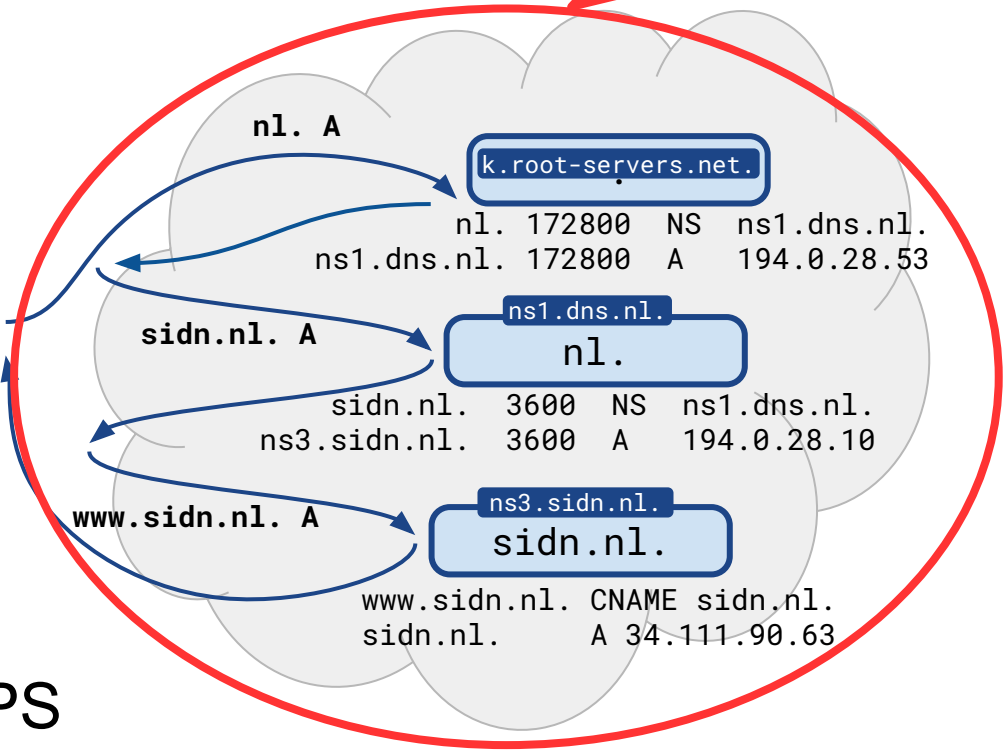
juli 2013 : RFC 6973
Privacy Considerations
for Internet Protocols

mei 2014 : RFC 7258
Pervasive Monitoring
is an Attack

Overal Encryptie

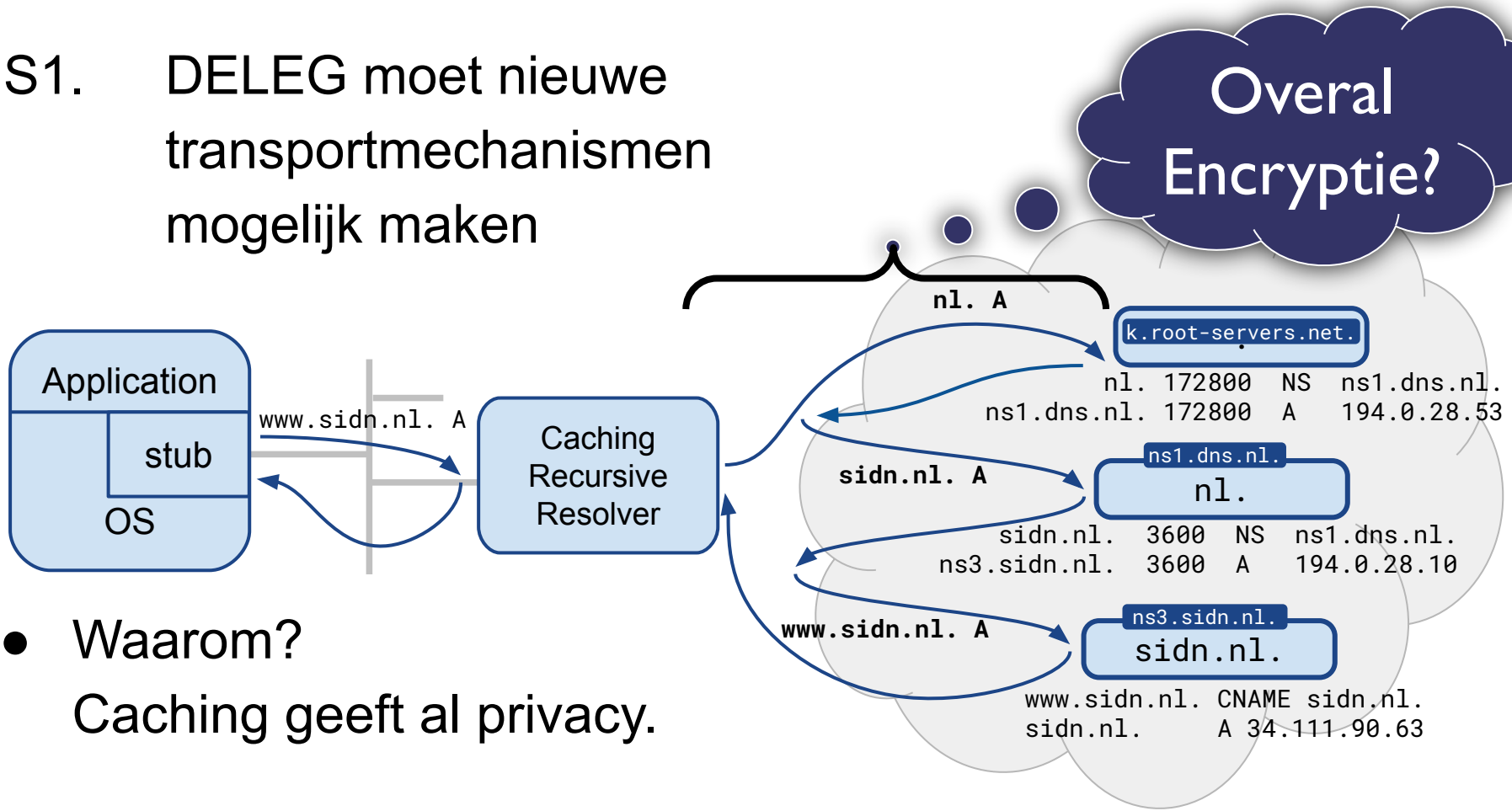
RFC 9156: minimaliseer (data in) queries





- DoT, DoH en DoQ
- RFC 7858: DNS over TLS
- RFC 8484: DNS over HTTPS
- RFC 9250: DNS over QUIC

S1. DELEG moet nieuwe transportmechanismen mogelijk maken



- Waarom?
  Caching geeft al privacy.

- Misschien RFC 7871: EDNS Client Subnet (ECS)?[ref]

H7. Meerdere onafhankelijke operators moeten een zone kunnen serven

- RFC 9460: Service Binding and Parameter Specification (de SVCB en HTTPS resource records)
- Komt voort uit de behoefte om browsers naar een operator door te verwijzen vanaf de apex van de zone
- `example.net. 3600 IN HTTPS 0 web-service.akamai.net.`
- 0 = AliasMode

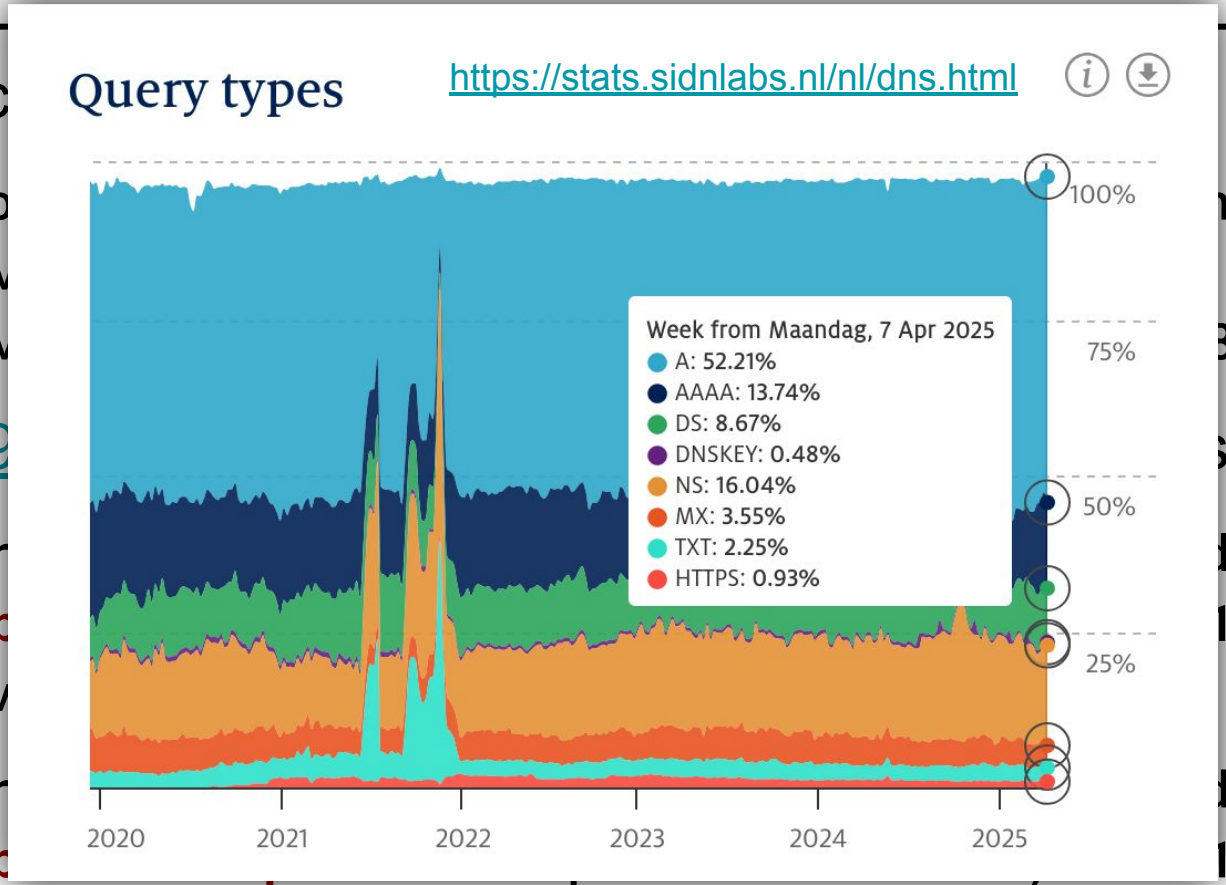
- `example.net. 3600 IN DELEG 0 dns-srv.cloudflare.com.`
  `DELEG 0 dns-service.godaddy.com.`
  `DELEG 0 dns-service.akamai.net.`

S1. DELEG moet nieuwe transportmechanismen mogelijk maken

- ServiceMode (alles > 0): container van key/value paren
- `ietf.org.  300  IN  HTTPS  1 . ( alpn="h3,h2"`
  `ipv4hint=104.16.44.99,104.16.45.99`
  `ipv6hint=2606:4700::6810:2c63,2606:4700::6810:2d63 )`
- RFC 9461: Service Binding Mapping voor DNS servers
- `_dns.resolver.arpa.  60  IN  SVCB  1 dns.quad9.net. (`
  `alpn="dot" port=853 ipv4hint=9.9.9.9,149.112.112.112`
  `ipv6hint=2620:fe::fe )`
- `_dns.resolver.arpa.  60  IN  SVCB  2 dns.quad9.net. (`
  `alpn="h2"  port=443 ipv4hint=9.9.9.9,149.112.112.112`
  `ipv6hint=2620:fe::fe dohpath="/dns-query{?dns}" )`

S1. DELEG moet nieuwe transportmechanismen mogelijk maken

- Servic paren
- ietf.o ="h3,h2"
  ipv
  ipv 310:2d63)
- RFC 9 servers
- _dns.r d9.net. (
  alp 12.112.112
  ipv
- _dns.r d9.net. (
  alp 12.112.112
  ipv6hint=2620:fe::fe dohpath="/dns-query{?dns}")

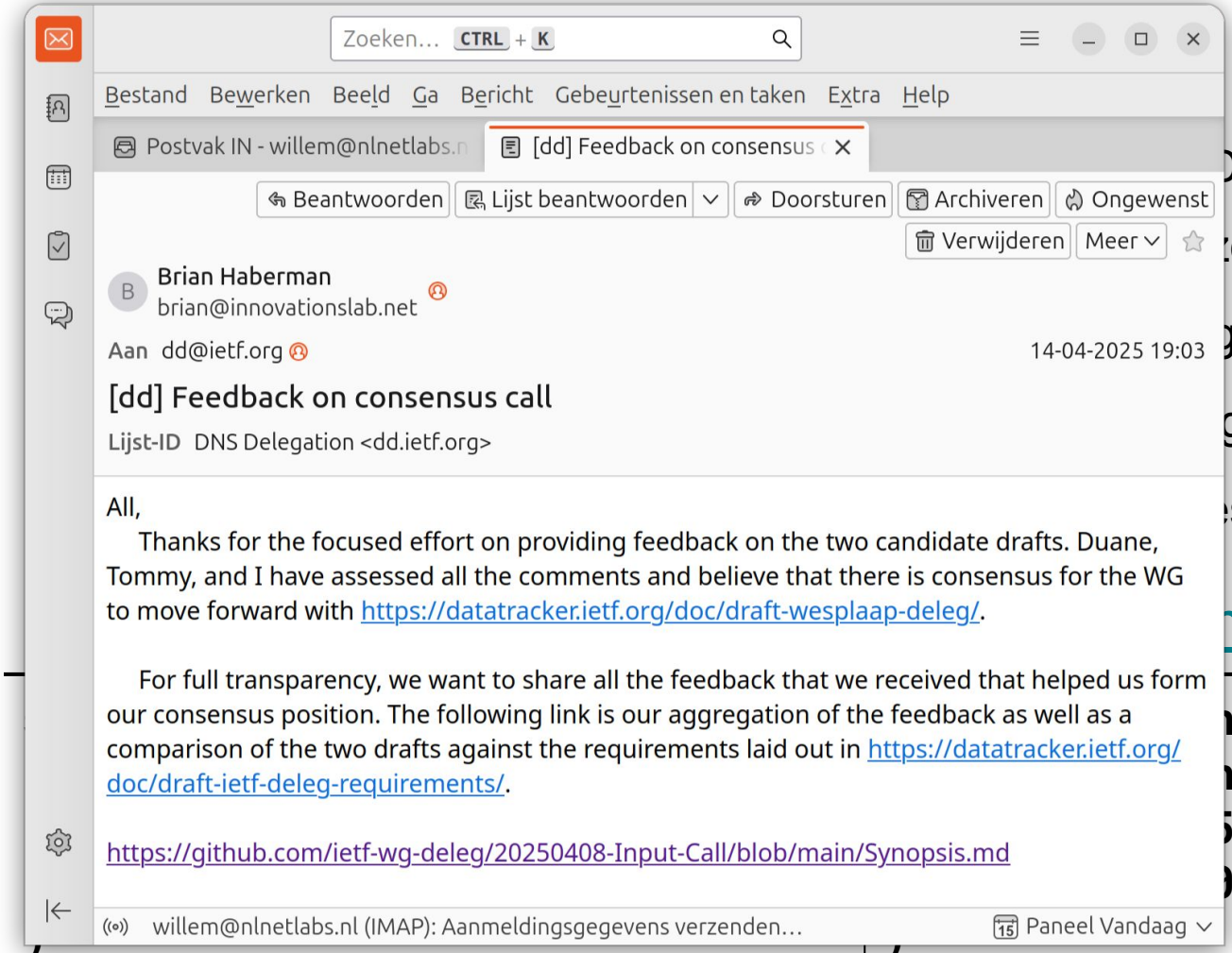


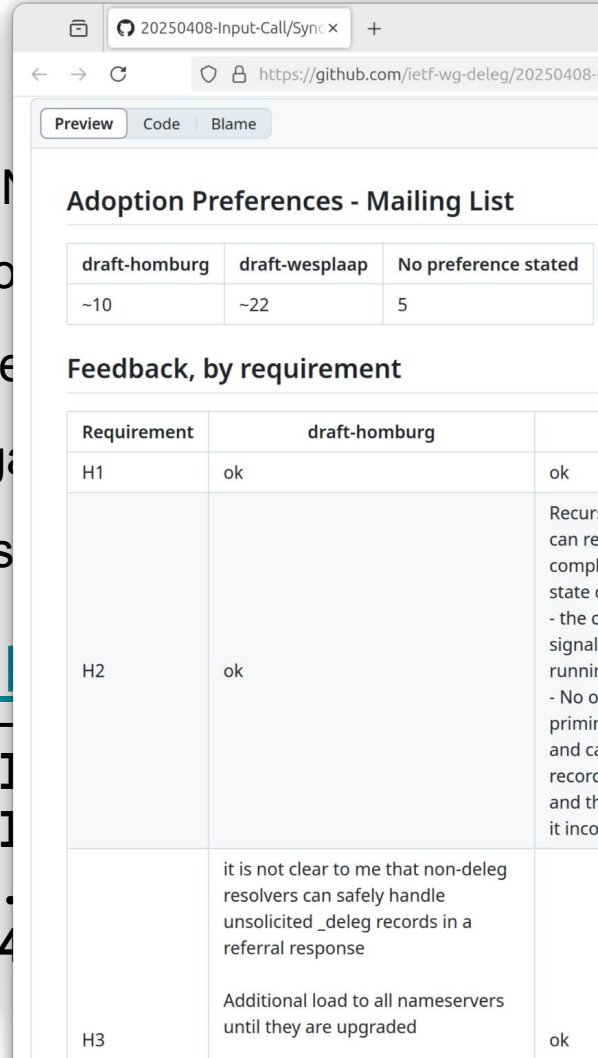
SVCB formaat ticks all the boxes

- H4. DELEG moet delegaties kunnen beveiligen met DNSSEC.
- H7. Meerdere onafhankelijke operators moeten een zone kunnen bedienen
- S1. DELEG moet nieuwe transportmechanismen mogelijk maken
- S2. DELEG moet alle benodigde details voor de delegatie bevatten
- S6. DELEG moet uitbreidbaar zijn met nieuwe functies

wesplaap-deleg	homburg-deleg

`sidn.nl DELEG (`
`1 ns5.sidn.nl. alpn="dot"`
`Glue4=145.40.68.55`
`Glue6=2604:1380:4601:6300::1`
`)`
	`sidn._deleg.nl IDELEG (`
	`1 ns5.sidn.nl. alpn="dot"`
	`ipv4hint=145.40.68.55`
	`ipv6hint=2604:1380:4601:6300::1`
	`)`


Zoeken… CTRL + K
Bestand Bewerken Beeld Ga Bericht Gebeurtenissen en taken Extra Help
Postvak IN - willem@nlnetlabs.n
[dd] Feedback on consensus
Beantwoorden
Lijst beantwoorden
Doorsturen
Archiveren
Ongewenst
Verwijderen
Meer
Brian Haberman
brian@innovationslab.net
Aan dd@ietf.org
14-04-2025 19:03
[dd] Feedback on consensus call
Lijst-ID DNS Delegation <dd.ietf.org>
All,
Thanks for the focused effort on providing feedback on the two candidate drafts. Duane, Tommy, and I have assessed all the comments and believe that there is consensus for the WG to move forward with https://datatracker.ietf.org/doc/draft-wesplaap-deleg/.
For full transparency, we want to share all the feedback that we received that helped us form our consensus position. The following link is our aggregation of the feedback as well as a comparison of the two drafts against the requirements laid out in https://datatracker.ietf.org/doc/draft-ietf-deleg-requirements/.
https://github.com/ietf-wg-deleg/20250408-Input-Call/blob/main/Synopsis.md
willem@nlnetlabs.nl (IMAP): Aanmeldingsgegevens verzenden…
Paneel Vandaag


20250408-Input-Call/Sync
https://github.com/ietf-wg-deleg/20250408-
Preview Code Blame
Adoption Preferences - Mailing List
draft-homburg draft-wesplaap No preference stated
~10 ~22 5
Feedback, by requirement
Requirement draft-homburg
H1 ok ok
H2 ok
H3 it is not clear to me that non-deleg resolvers can safely handle unsolicited _deleg records in a referral response
Additional load to all nameservers until they are upgraded
ok

DELEG na de keuze

- DNSSEC uitbesteden aan de operator
  draft-homburg-deleg-incremental-dnssec

```
$ORIGIN example.
@           IN  SOA    ns zonemaster …
customer4   IN  DELEG 1 ( ns.operator1
                dnskeyref=customer4.keys.operator1 )
            IN  DELEG 1 ( ns.operator2
                dnskeyref=customer-keys.operator3 )
```

- Een reeks RR typen autoritatief aan de ouder zijde
  draft-arends-parent-only-record-signalling

```
customer4   IN  DELEG       1 ns.operator1
            IN  DNSKEYREF   customer4.keys.operator1
```

DELEG: DNS op de schop

- Genoeg energie in de (IETF) DNS gemeenschap
- Maar echt heel veel veranderingen nodig
  - Behalve alle DNS software ook de registratiesystemen van registries en registrars!
- Krijgen we een soort situatie vergelijkbaar met IPv6?
- Heeft dit kans van slagen? DNS werkt toch gewoon?

WDJ?

NLNETLABS
Willem Toorop
willem@nlnetlabs.nl