

Connect by Name



NLNETLABS
Benno Overeinder



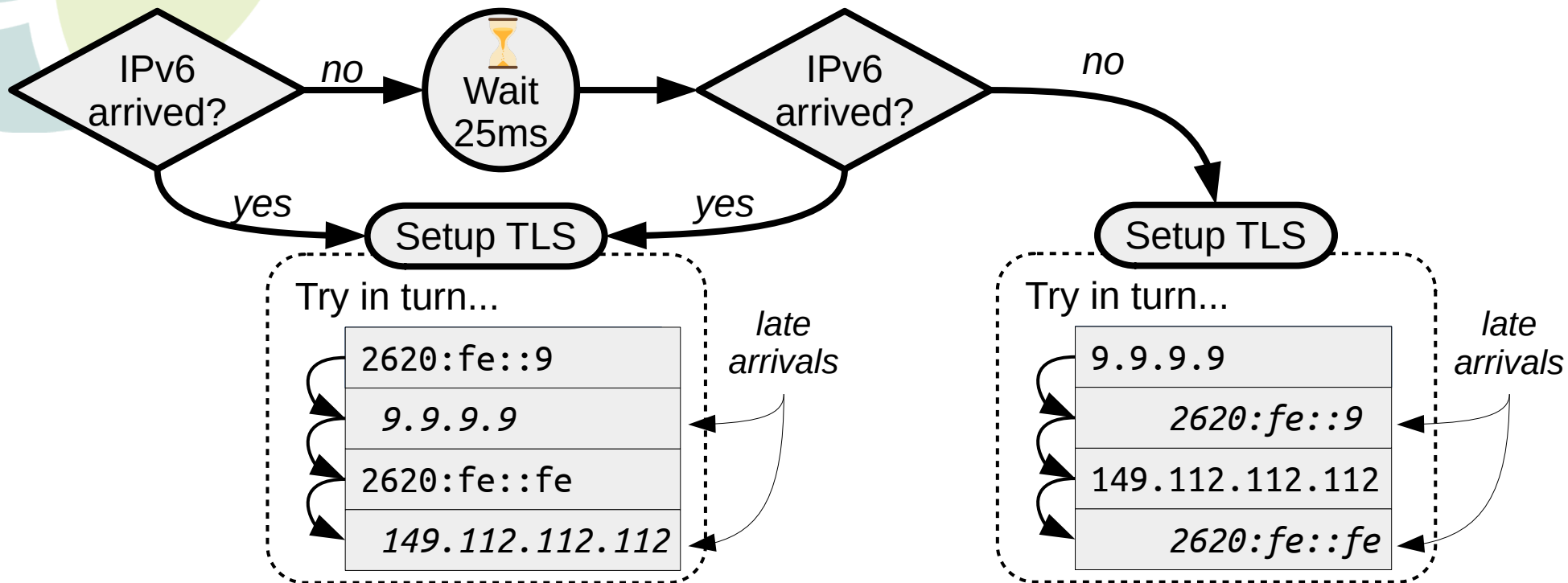
What does it mean to setup a connection?

- Using modern standards...
- Securely
- Privately

```
c = connectByName("dns.quad9.net", "doh");
```

Step 1: Happy Eyeballs

- Lookup IPv6 of dns.quad9.net
 - Lookup IPv4 of dns.quad9.net
- } *Simultaneously*



DNSSEC

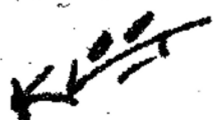
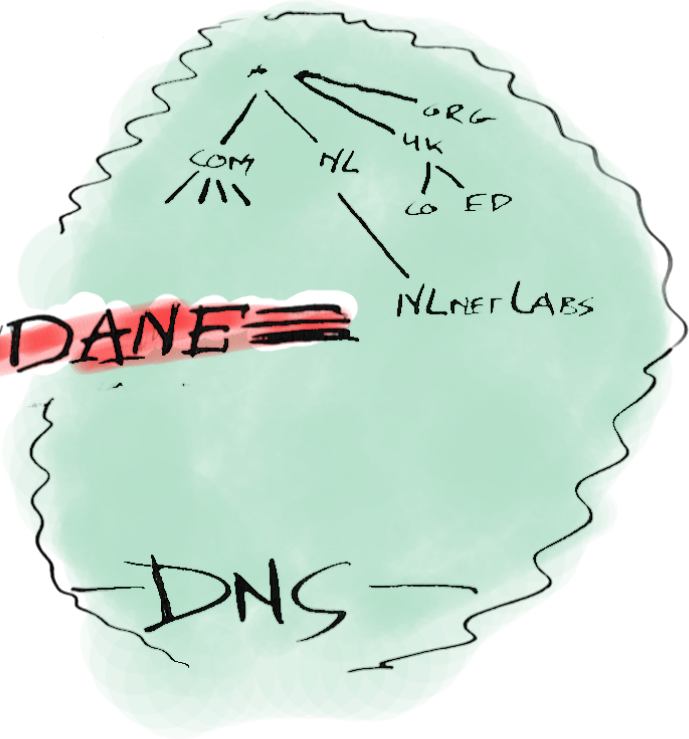
```
willem@makaak: ~  
willem@makaak:~$ dig dns.quad9.net AAAA +dnssec  
  
; <<>> DiG 9.16.6-Ubuntu <<>> dns.quad9.net AAAA +dnssec  
;; global options: +cmd  
;; Got answer:  
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 11598  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1  
  
;; OPT PSEUDOSECTION:  
; EDNS: version: 0, flags: do; udp: 4096  
;; QUESTION SECTION:  
;dns.quad9.net.                IN          AAAA  
  
;; ANSWER SECTION:  
dns.quad9.net.                994        IN          AAAA       2620:fe::9  
dns.quad9.net.                994        IN          AAAA       2620:fe::fe  
dns.quad9.net.                994        IN          RRSIG     AAAA 8 3 1200 20201223190000 202  
01206190000 61069 quad9.net. PWVs+67FpGquaK4uGFr3qVyRh58ibFSVB+RPLFRQjIkoMr/iIVw  
LVwD3 MSKLhsz53TTZU48ZCwP9CpMbCmTxsD4at4I5xUgkfkftq6XQLHhLDfa ZAhUashRaP3945Wq1  
Kxy8C6hTU3HLZCJVAXaRm6JavL/4jzNxYohAiGa cQM9W84QJTfjr8WLG4wYmEKpX6WBmXd2R85C7UNU  
LKke7Y7wGktQZkd+ 7xLvnKJCuzvqj5/0mLytZkwL2BeK9pSXG1y08fvdWJTLmpbi/7nNnn6I FvfXXL  
FiCKBVKEhu5uFJRLe/GFynhrxWJE45nR6hLIj3qylkp0/L8mgn Yyfgdg==  
  
;; Query time: 8 msec  
;; SERVER: fd06:5431:4e7b::1#53(fd06:5431:4e7b::1)  
;; WHEN: wo dec 09 12:46:17 CET 2020  
;; MSG SIZE rcvd: 395  
  
willem@makaak:~$
```

DANE



DANE

HIM

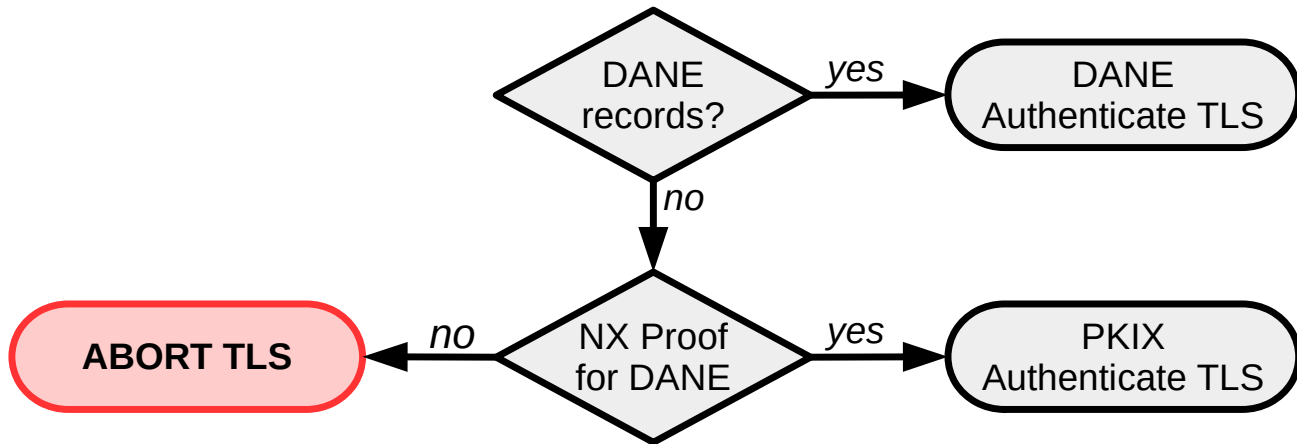


Happy Eyeballs, DNSSEC & DANE

Step 1:

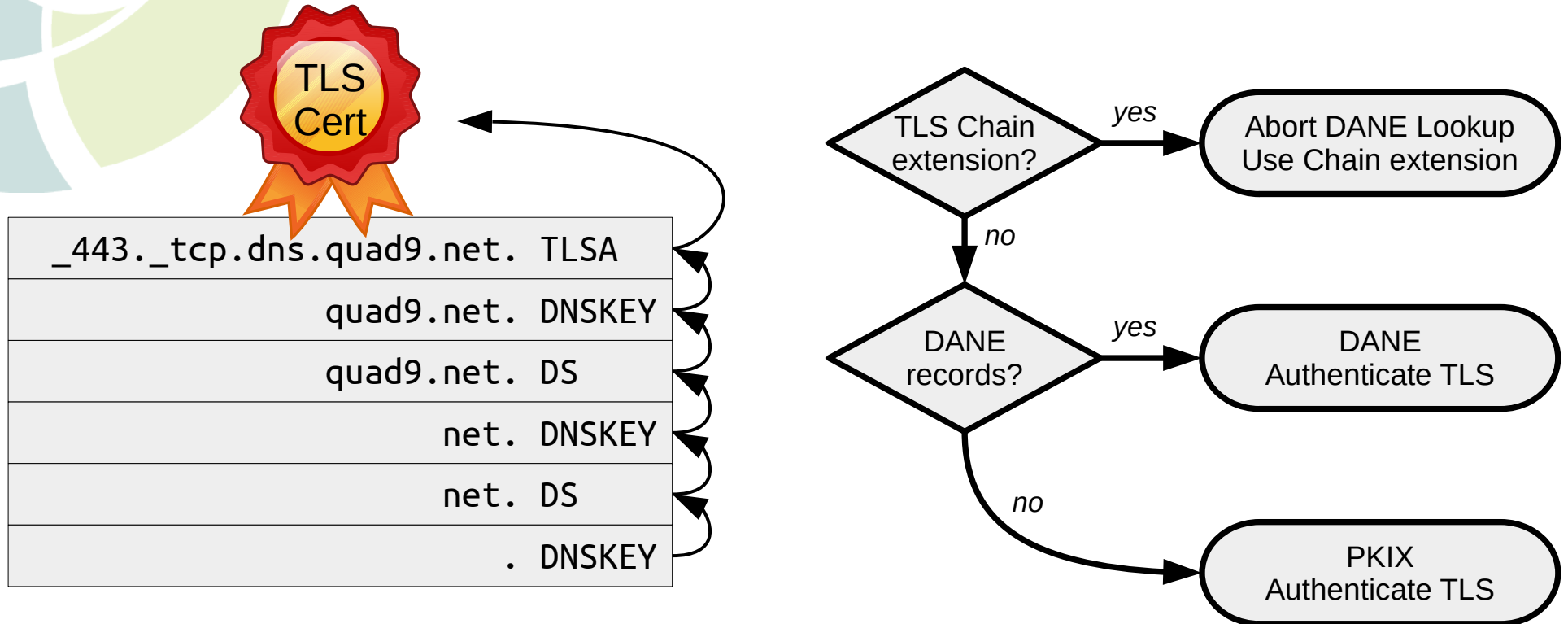
- Lookup IPv6 of dns.quad9.net +dnssec
- Lookup IPv4 of dns.quad9.net +dnssec
- Lookup _443._tcp.dns.quad9.net TLSA +dnssec

Simultaneously



DNSSEC Chain TLS Extension

- DANE Embedded in the TLS Handshake:



Zero config DNSSEC

System requirement
for DNSSEC:




root KSK

*validate with
ICANN CA*

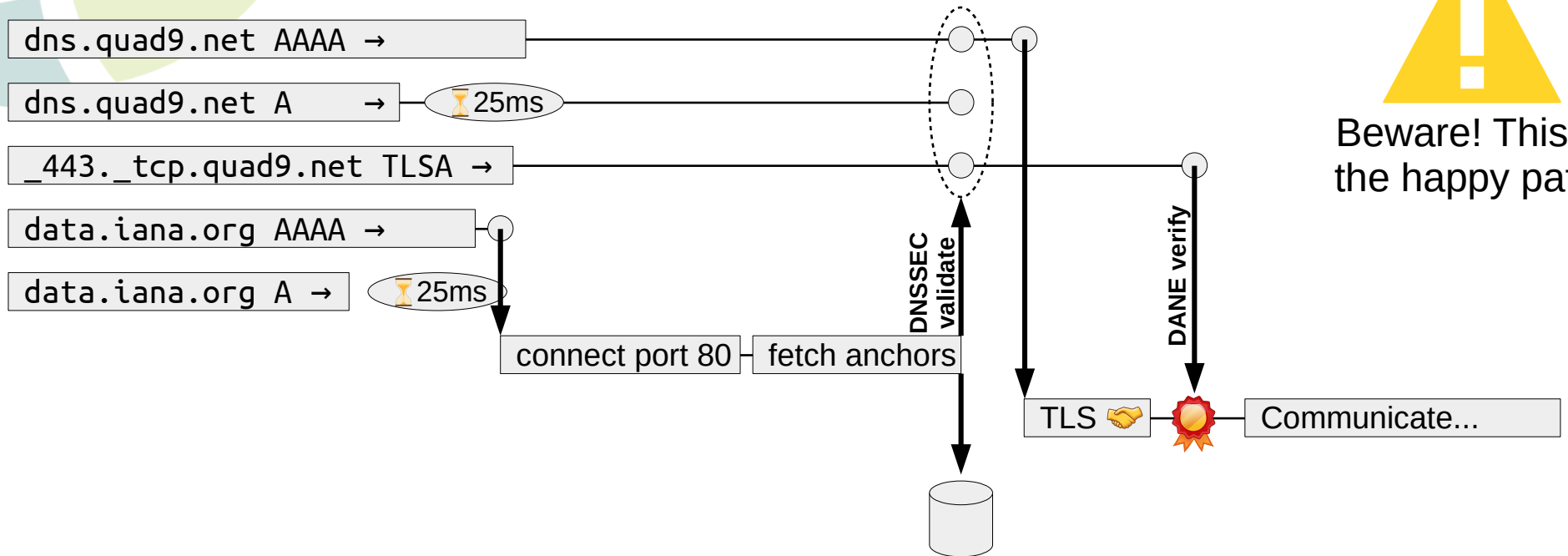
Alternatively, from application fetch:
[RFC7958](#)

A screenshot of a web browser window showing the index of root anchors. The browser address bar displays "data.iana.org/root-anchors/". The page content is a table with columns for Name, Last modified, and Size. The table lists several files, including "root-anchors.p7s" and "root-anchors.xml". An arrow points from the "root-anchors.xml" link in the table to the "root KSK" caption in the left column.

Name	Last modified	Size
Parent Directory		-
old/	2018-12-19 20:10	-
checksums-sha256.txt	2018-12-20 20:33	248
icannbundle.pem	2017-02-03 00:00	13K
root-anchors.p7s	2018-12-20 20:33	4.1K
root-anchors.xml	2018-12-19 22:03	690



Happy Eyeballs, DNSSEC & DANE + fetching/renewing DNSSEC TA Step 1:



Beware! This is the happy path.



DNS-over-TLS (DoT) DNS-over-HTTPS (DoH)

- Do all DNS lookups *privately*
- Setting up DoT or DoH in itself involves:
 - Happy Eyeballs
 - DANE Authentication
 - With DNSSEC Chain, or
 - DANE records acquired over the as of yet unauthenticated DoT or DoH session



Much, much, more ...

- DNSSEC Roadblock avoidance RFC8027
- DNSSEC with DNS64 / NAT64 RFC7050
- DNS-over-Quick (DoQ)
- Oblivious DNS-over-HTTPS (ODOH)
- Multiple Provisioning Domains RFC7556
- etc.

What does it mean to setup a connection?

- Using modern standards...
- Securely
- Privately



What is Connect by Name?

Turn this:



Into this:

