DNS, SNI, TLS, HTTPS: Modern DNS & Privacy

@PowerDNS_Bert
bert.hubert@powerdns.com

POWERDNS
AN OX COMPANY

The domain name system

[8] J. Postel, "Internet Name Server", IEN 116, USC/Information Sciences Institute, August 1979.

IEN 116

J. Postel
ISI
August 1979

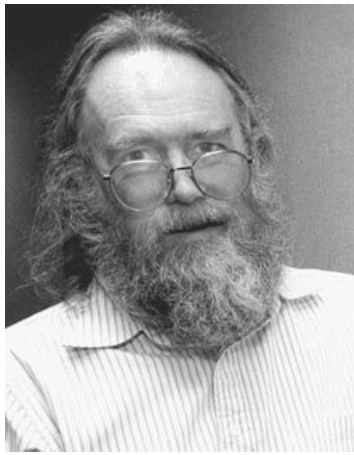
Obsoletes: 89, 61

INTERNET NAME SERVER

INTRODUCTION

This memo defines the procedure to access an Internet Name Server. Such a server provides the actual addresses of hosts in the internet when supplied with a host name. An Internet Name Server is a dynamic name-to-number translation service.

This server utilizes the User Datagram Protocol (UDP) [2], which in turn calls on the Internet Protocol (IP) [3].



DNS is the last plaintext protocol on the internet.

(or is it?)

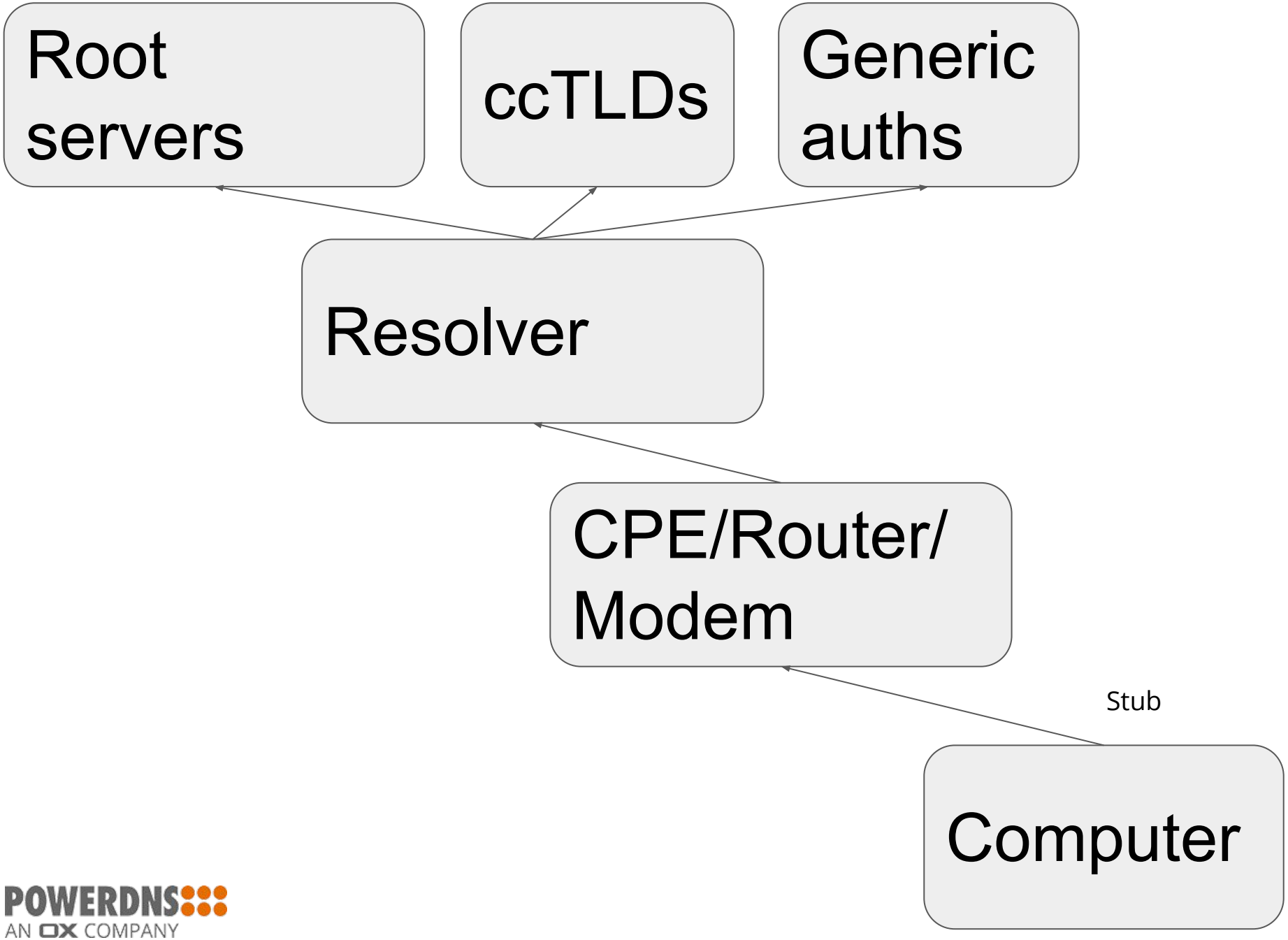
Fiscus vindt bellen met Zwitsers al verdacht

Door **LEON BRANDSEMA & BART MOS**
15 apr. 2019 in GELD

Lees voor

AMSTERDAM - De Belastingdienst houdt mensen tegen het licht die afgelopen jaren telefonisch contact hadden met de Zwitserse bank Credit Suisse. De fiscus vraagt daarbij om „kopieën van alle correspondentie" met de Zwitsers.

Volgens de Belastingdienst hebben twee Credit Suisse-klanten een brief ontvangen.



1998-2015 (development):

DNSSEC: Complex **message** integrity with negative privacy impact

2009:

DNSCurve/DNSCrypto: simple encrypted DNS **transport** with privacy

2015:

DNS over TLS. “Simple” encrypted DNS **transport** over port 853

2018:

DNS over HTTPs. “Simple” encrypted DNS **transport** over real HTTPs on port 443

- *With cookies and tracking*

And then.. Network operators & operating system vendors did nothing.

Except suddenly: American browser vendors & CDNs decided to fight for our privacy!

Metadata privacy leaks:

- HTTP attempts
- *DNS lookups*
- eSNI
- OCSP
- IP address

eSNI: Attempting the near impossible
.. work in progress

New trust model: Browser talks straight to the CDN, bypassing your network & your security settings

May break:

- Security filtering
- Security monitoring
- CDN performance
- Split horizon / VPN
- Your privacy (?!)

- Enterprise impact: who controls your network?
  - Endpoints harder and harder to manage
  - Management from network is going away

- Trust the cloud?

- US providers adhere to FISA 702 which does not protect privacy of Europeans at all
- **Can’t fix that in Mozilla, Google or Cloudflare privacy policy**
- US Cloud Act means US companies can’t shield their European servers
- So to enhance our privacy, we must first break it
- DNS traffic tells everything about you

Rationale:

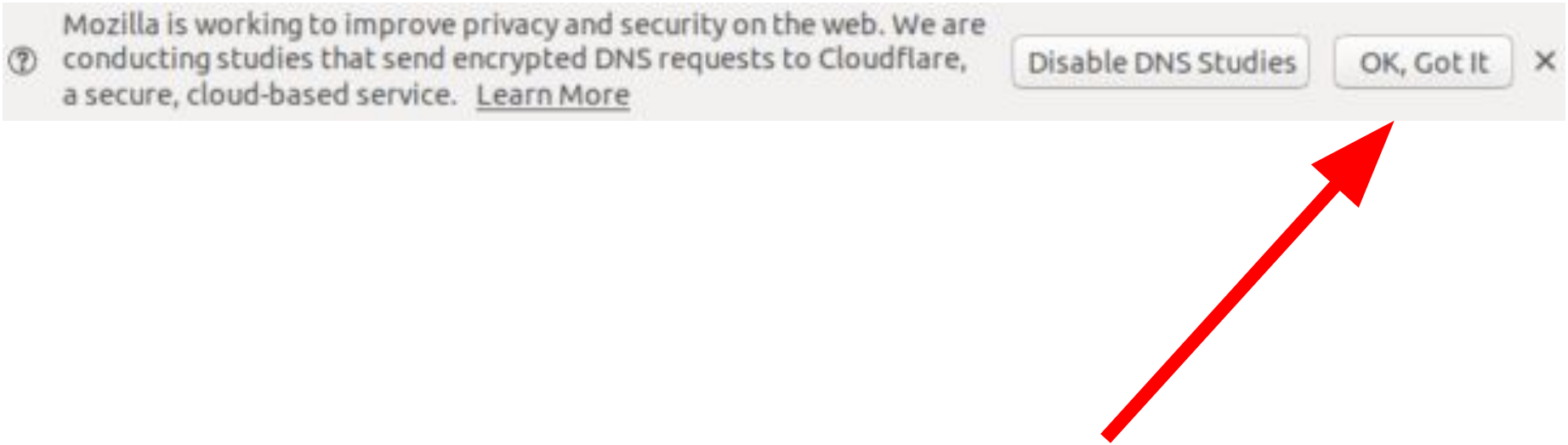
- NXDOMAIN redirection
- Turkish/Chinese/Russian freedom fighters
- Countries with no privacy regimes
- Must get “everyone” on DoH to provide cover & impact

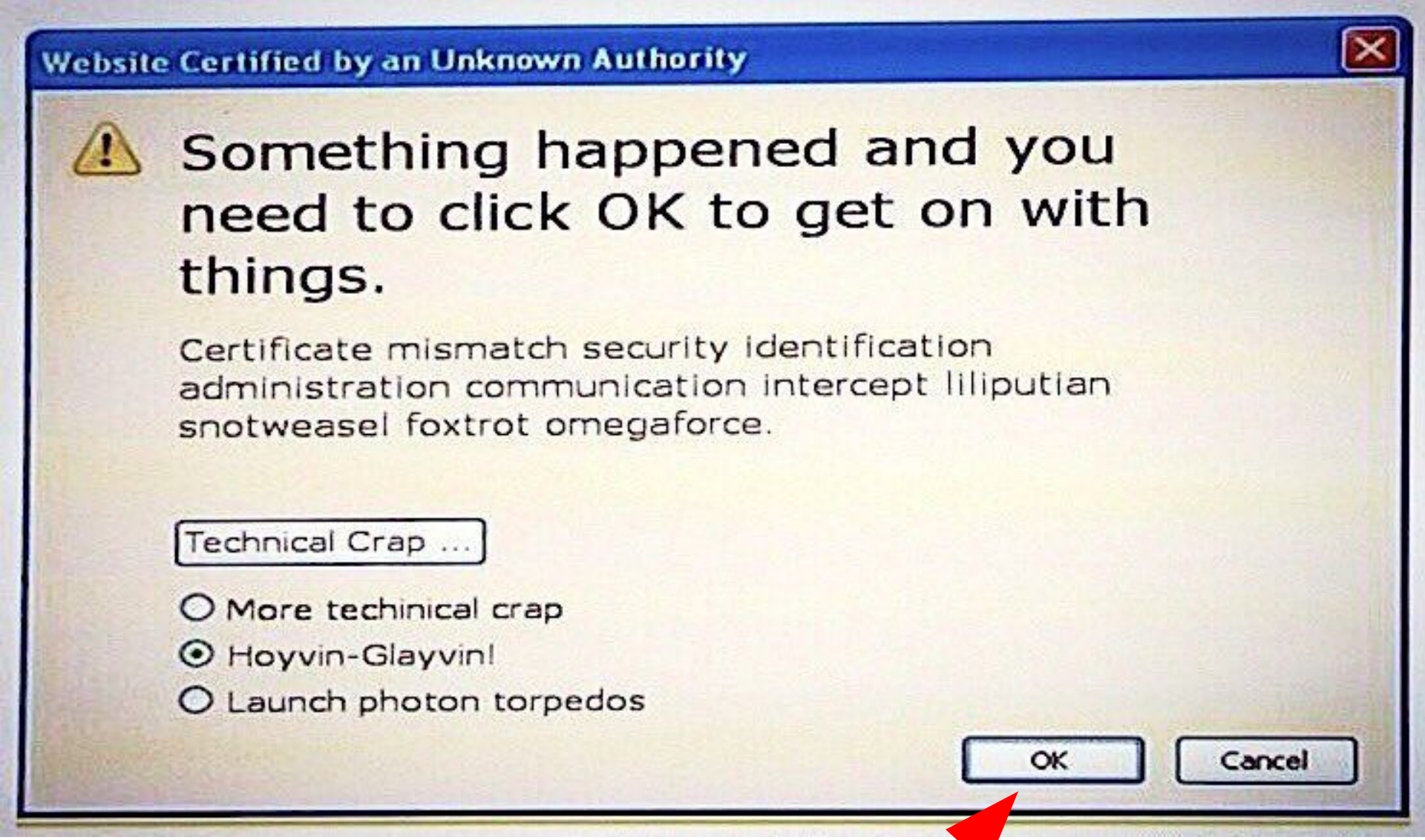
Mozilla:

“We have implemented DNS over HTTPS and would like to deploy it by default for our users.

The user will be informed that we have enabled use of a TRR and have the opportunity to turn it off at that time, but will not be required to opt-in to get DoH“

https://mailarchive.ietf.org/arch/msg/doh/po6GCAJ52BAKuyL-dZiU91v6hLw


Mozilla is working to improve privacy and security on the web. We are conducting studies that send encrypted DNS requests to Cloudflare, a secure, cloud-based service. Learn More
Disable DNS Studies
OK, Got It



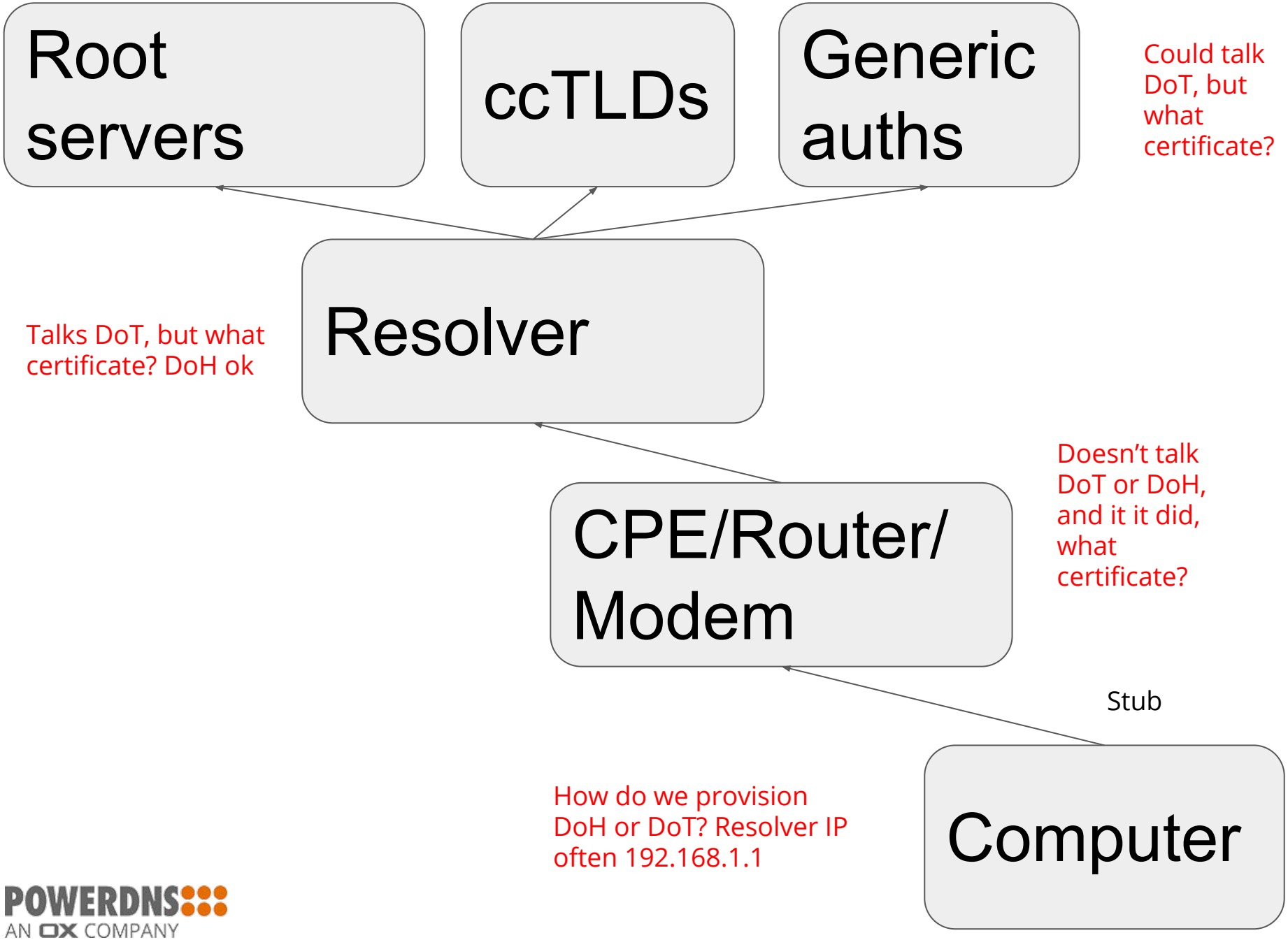
Google:

- Will attempt DoT already, will attempt to do DoH if provider offers it and publishes somehow
- Will not surprise users with sudden changes
- However, capability is there to have users opt-in. *Users might be nagged about this if provider offers no encryption, no DNSSEC or messes with DNS.*

https://mailarchive.ietf.org/arch/msg/dns-privacy/kpt6ZYMN5H3DsXPVi_QIdmbAqJw

What to do?

- Turn on DNS over TLS on your resolvers, see Android phones use it!
  - And likely Chrome later
- Run DoH, will not see any use, but practice is good
  - Discovery is a problem
- Get involved with standardisation
  - Enough open problems



Summarising

- **We need encrypted DNS**
- But please not by default to third parties outside of our control

DNS, SNI, TLS, HTTPS: Modern DNS & Privacy

@PowerDNS_Bert
bert.hubert@powerdns.com

POWERDNS
AN OX COMPANY