Council of European National
Top-Level Domain Registries

DoH!

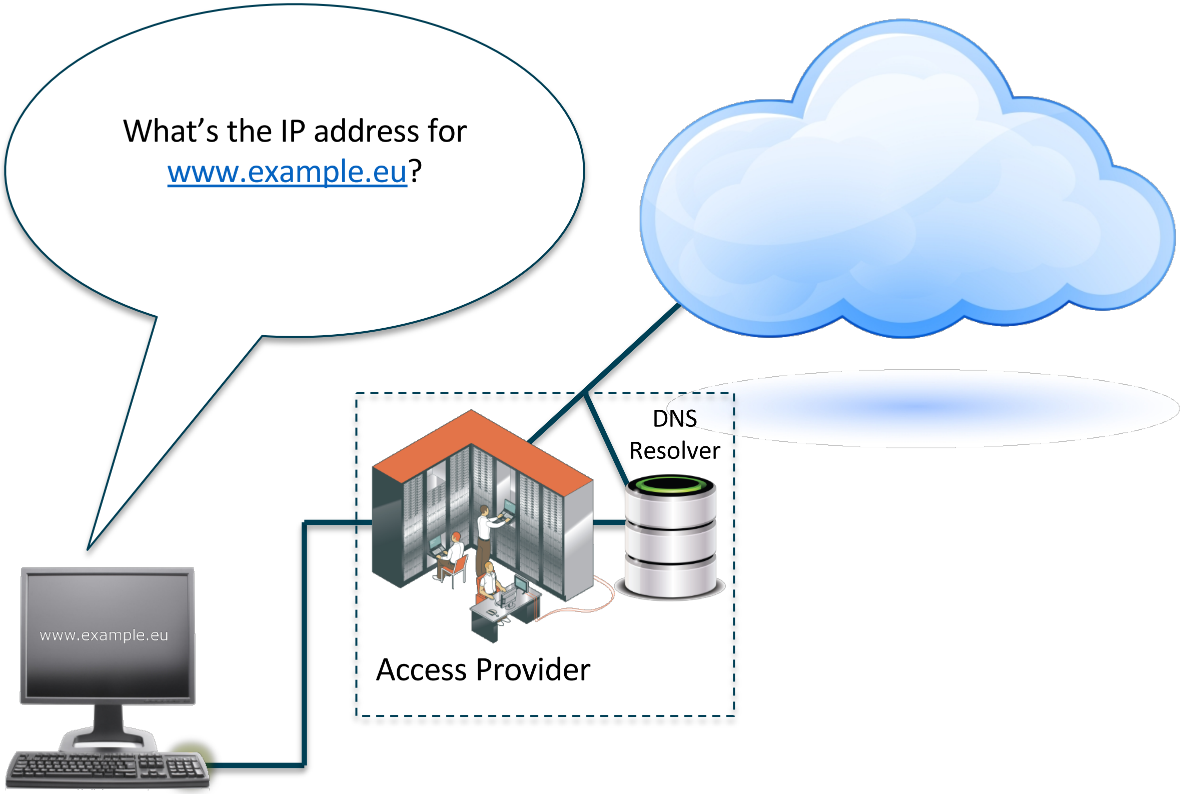
Peter Van Roste
peter@centr.org

GAC/ccNSO meeting - ICANN 64
Kobe, Japan
13 March, 2019

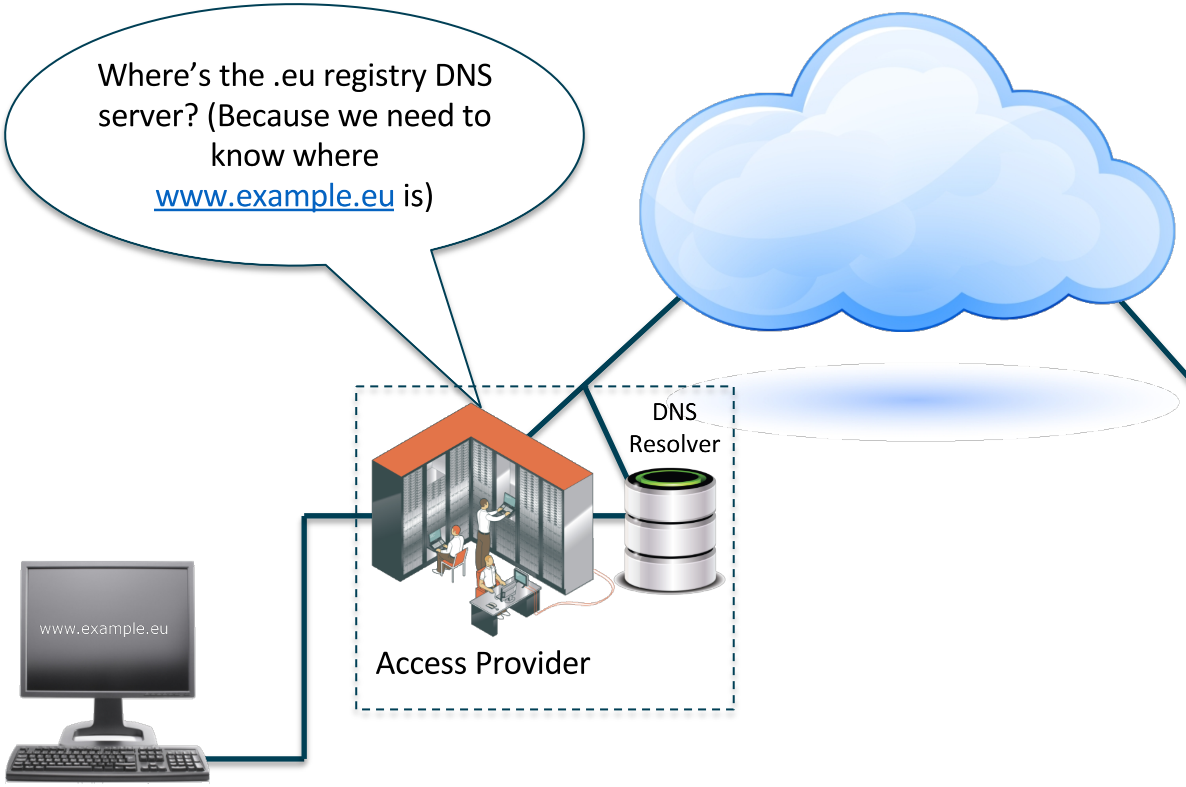
Who knows what DoH is?

Council of European National
Top-Level Domain Registries

Today: Operating System asks Access Provider for IP address of www.example.eu

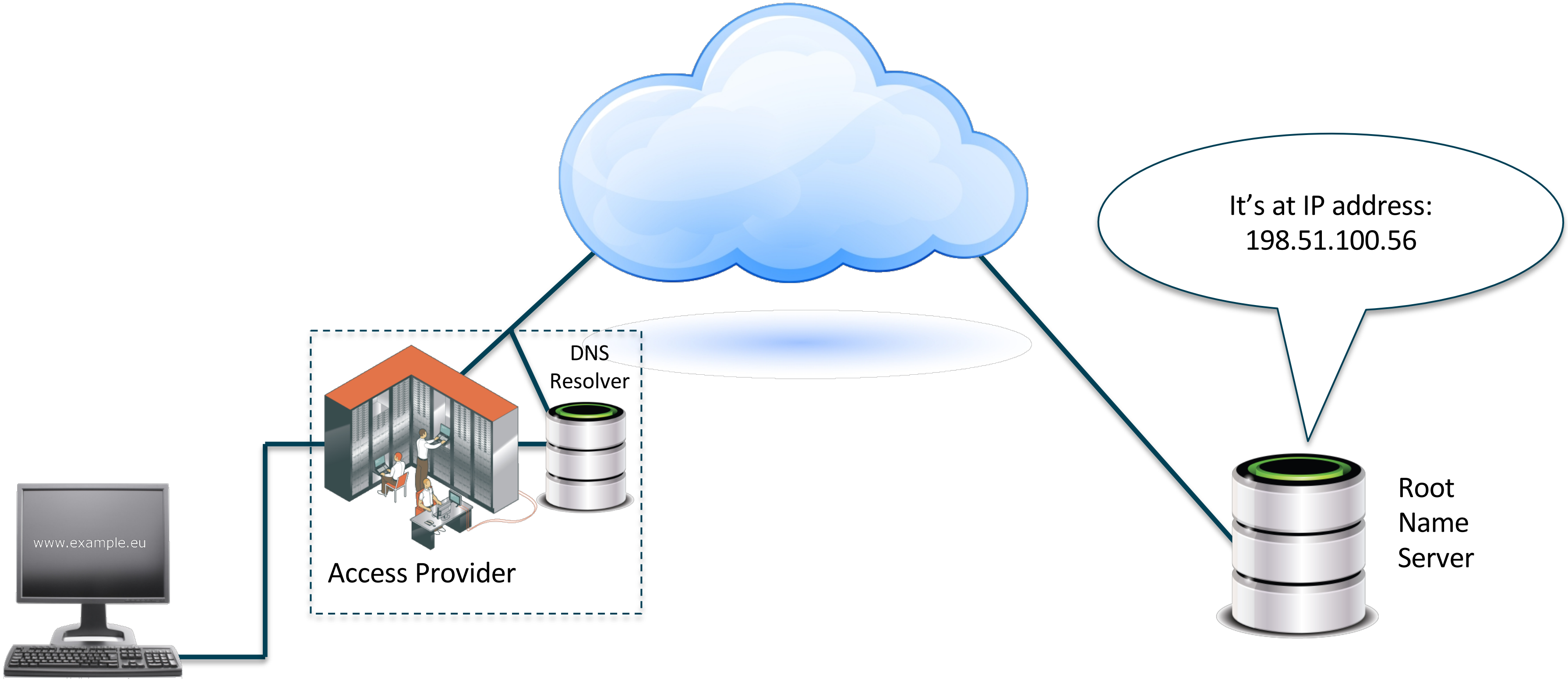


Today: DNS Resolver asks Root Name Server for IP of a DNS server for .eu


Where's the .eu registry DNS server? (Because we need to know where www.example.eu is)
DNS Resolver
www.example.eu
Access Provider
Root Name Server

Council of European National
Top-Level Domain Registries

Today: DNS Resolver asks Root Name Server for IP of a DNS server for .eu

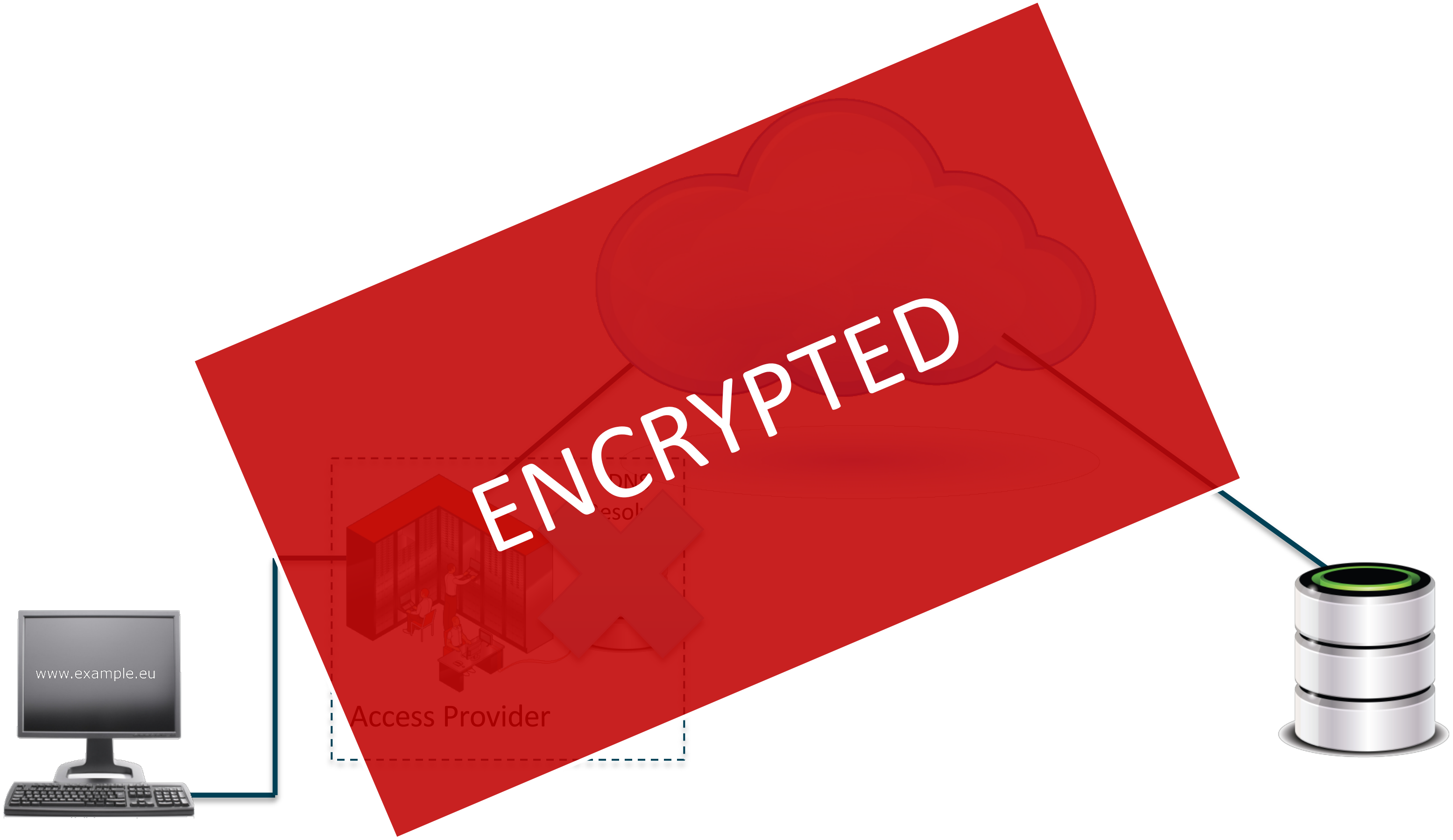


What is DoH

- DNS over HTTPS
- It’s a protocol (in an RFC standard) that allows resolving a domain name in a different way than we are used to
  - Rather than your ISP (or company) resolver, your browser will take care of resolving a domain name.
  - Your browser will work with a selected service provider (e.g. 1.1.1.1) to answer those queries.
  - Only a few organisations can provide robust reliable resolving services to the whole world.
  - Browsermarket: Chrome 64.63% + Internet Explorer 10.49% + Firefox 9.83% + Edge 4.3% + Safari 3.79% = 93.04%

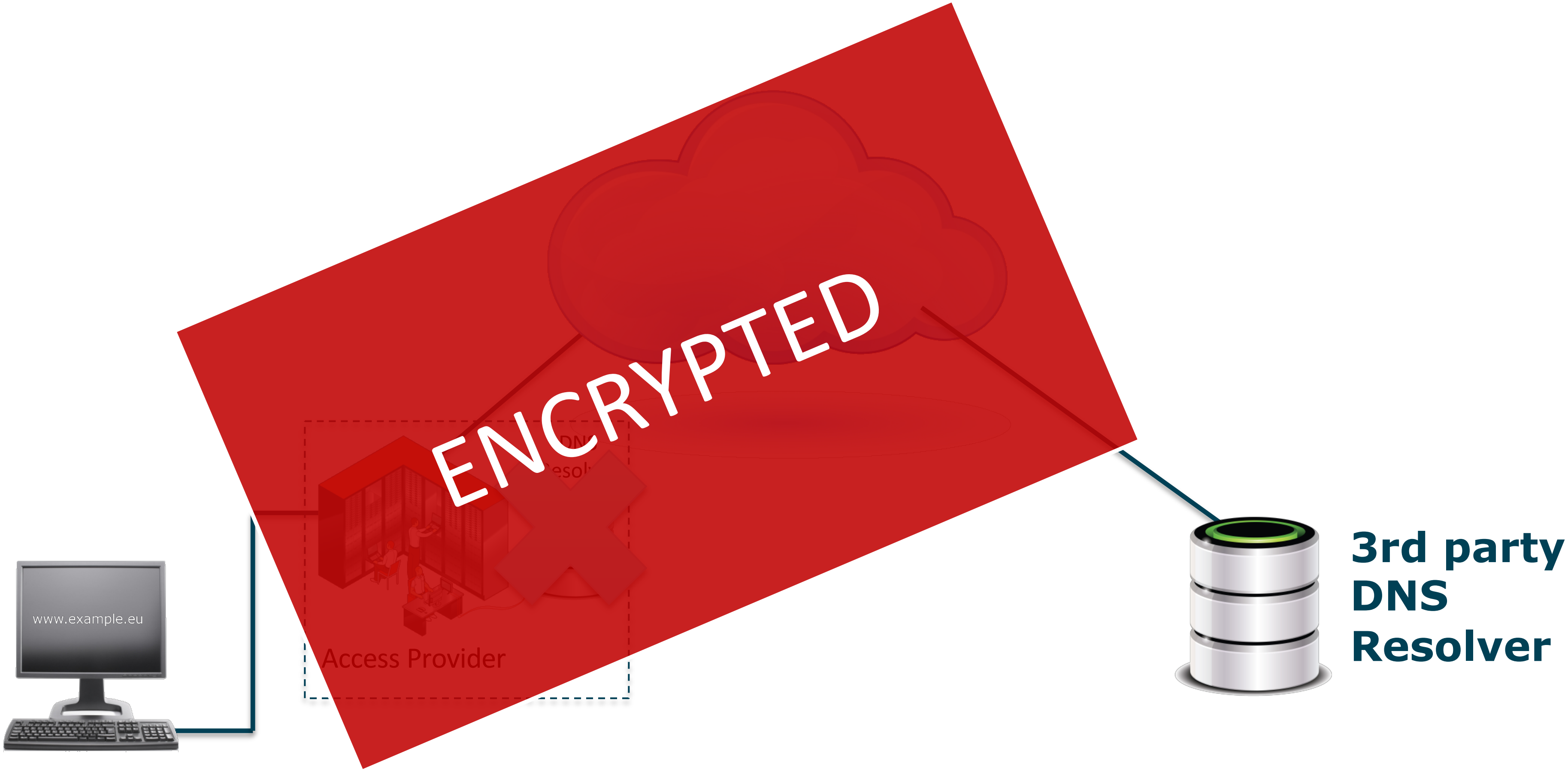
    (Source: NetApplications.com © 2017)

What does it look like?



3rd party DNS Resolver

What does it look like?



Why the change?

- DoH hides DNS traffic in HTTPS traffic, making it unblockable.
- Some well known security and privacy issues with regular DNS resolving have been unaddressed for 3 decades
  - Clear text queries
  - (wo)Men-in the middle attacks
- DoH provides answers by encrypting DNS requests and responses and securing the path between user and DNS resolver

Who likes it?

- Users (Art. 19) cautiously positive: more privacy
- Pirates and journalists in oppressive regimes: no blocking
- Browser vendors: more control
- Selected resolvers: more juicy data (even though they will remove PII after 24 hours and will never ever ever use or sell data)

Who hates it?

- Users that don’t like a central control point or users that trust their local ISP more than a third party (foreign) resolver
- ISPs:
  - losing control over network traffic
  - Losing juicy user data
  - Losing ability to stop abusive traffic
- Some DNS service providers: losing control and data (and business)
- Probably (if they realise the impact) law enforcement: losing data available in their jurisdiction
- Probably (if they realise the impact) Courts: who to send blocking order to?
- Organisations like Internet Watch Foundation or those providing parental control tools

Who worries?

- CERTS:
  - Security (no visibility) and privacy (non-EU resolver?) concerns
  - Technical issues (e.g. resolving local names for a company's intranet)

Unresolved questions

- What impact would it have on user experience?
  - Would a Firefox user see the same thing as a Chrome user?

    Knock, knock. "Who's there?" - "The end of internet universality."
  - Will DoH be a baked-in resolving method or will users be able to choose between DoH and old-fashioned DNS resolution?
  - Will browsers hardcode resolvers in their software?
  - What would be the impact of a German court order sent to e.g. US-based resolver for a Belgian user?

- How will this change the balance of power in the DNS industry?
  - What if the resolvers disregard (voluntary!) standards?
  - What happens to ICANN if a handful of resolvers could decide to shape the rootzone as they see fit (e.g. adding .amazon)?

Impact on ccTLDs

- Limited **<u>on a technical level</u>**
  - Probably a decreased query load.
  - Need to be watchful things like TTL are respected by the resolvers, but limited power to enforce that.
  - Should make the DNS a little faster (even though tests have shown that a particular resolver is slower in responding to queries for content that are not in that resolver's cloud).
- Main impact: political/policy: the balance in the ecosystem will be affected

Any questions?

peter@centr.org

What is DoT

- DNS over TLS
- It’s a protocol (in an RFC standard) that allows resolving a name in a different way than we are used to
- The goal of the method is to increase user privacy and security by preventing eavesdropping and manipulation of DNS data.
- Similar to DoH but easier to block as it has a dedicated port
    - (DoH blocking would block all website traffic)
- Still a race between DoH and DoT but browsers will be calling the winner very soon. (and it is unlikely to be DoT)