Encrypted DNS in DTs Network: Status and Outlook

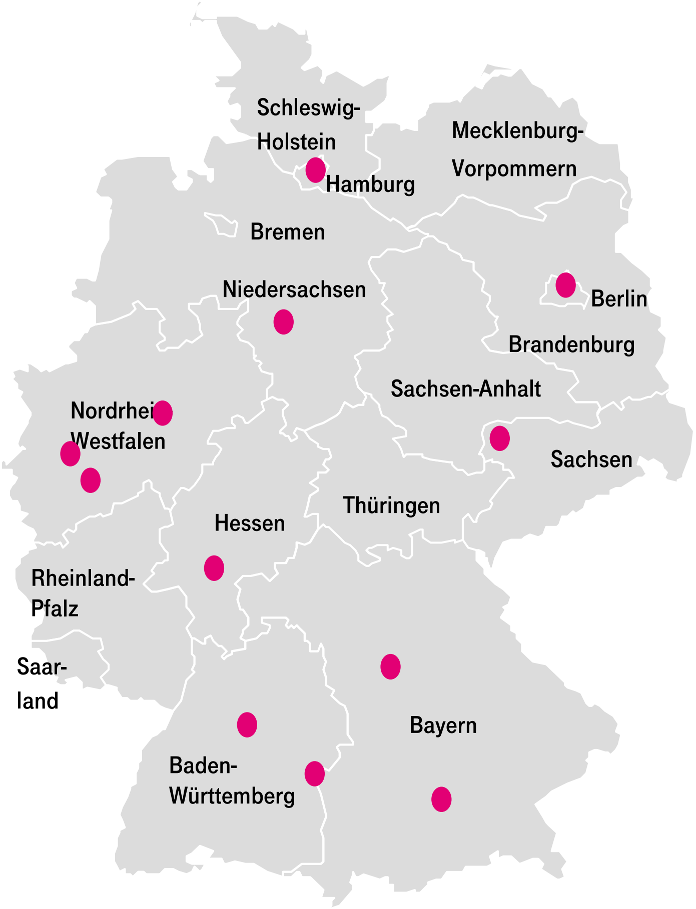
DNSOARC Lighting Talk (OARC41)

Nicolai Leymann | Berlin/DaNang | 04.09.2023

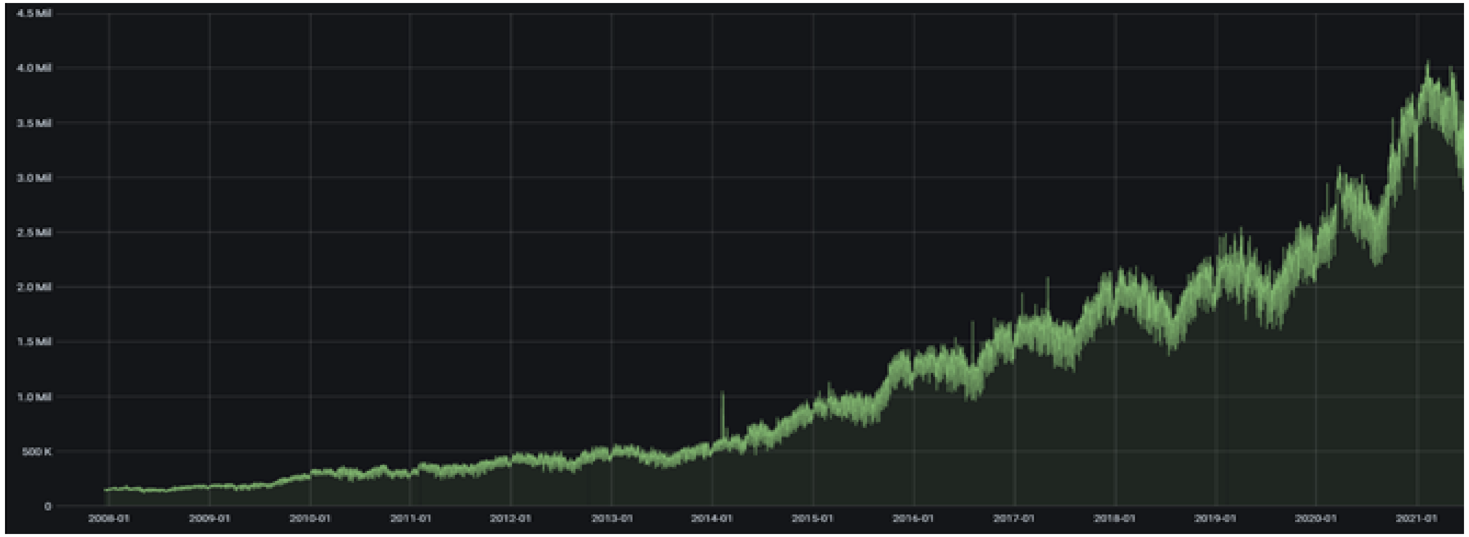
LIFE IS FOR SHARING.

Deutsche Telekom DNS Platform (Germany)

DT runs a large, high performance distributed DNS infrastructure, fully redundant IPv4/IPv6 enabled.



More than four Million DNS requests per second are handled



The DT DNS platform is the foundation for implementing a wide variety of user services. Those services REQUIRE that end users are using the DT DNS infrastructure. This includes security features, NAT64/DNS64 in Mobile Networks, Load Balancing for CDNs, ...

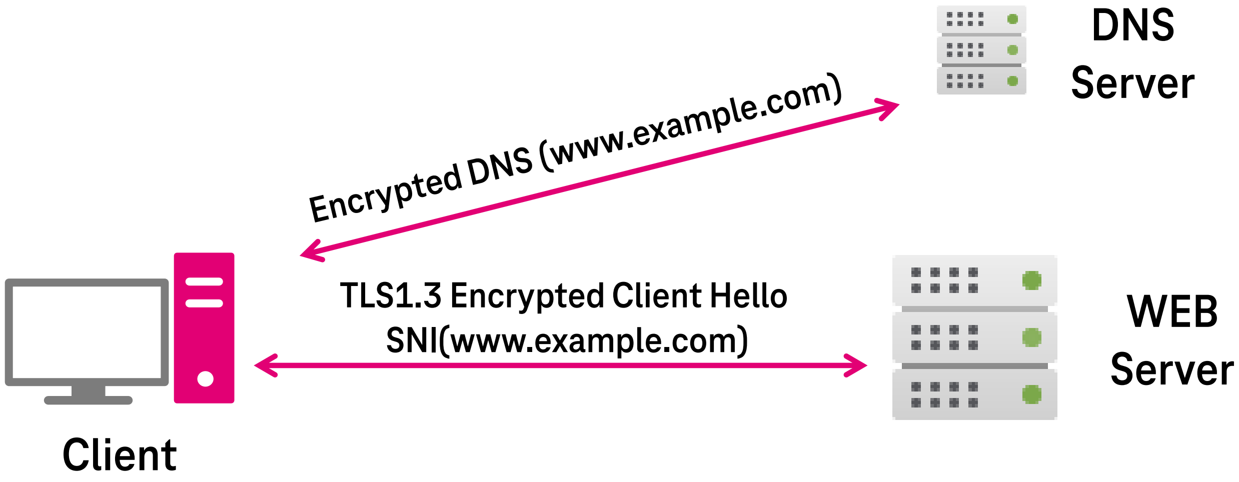
Deutsche Telekom DNS Platform (Germany)

- **Highly distributed platform covering fixed network and mobile network**
  - Separate servers due to different requirement in mobile network (e.g., NAT64, landing pages, …)
  - No anycast, we assign up to four IP addresses to clients (fixed network)
- **IPv4/IPv4 enabled, IPv6 preferred as transport for DNS**
  - default, DT supports Dual Stack for all customers for more than 10 years
- **End users are not forced to use DTs DNS (free to configure alternative DNS)**
  - 95% of users using DT DNS platform (only limited number of users know DNS)
- **Large project on investigating into encrypted DNS (DoT and DoH) about two years ago**
  - Not only Germany but across all NatCos
  - Major challenge: Wide variety of deployments and platforms
  - Goal: Enable encrypted DNS Group Wide
- **Implementation of encrypted DNS about two years ago (Germany)**
  - Support of DoT and DoH in fixed network
  - Support of DoH in mobile network (challenge: DoT probing in mobile networks, better use discovery)
  - Main benefit for small business products, not so much for classical home users

Challenges / Next Steps

- **DNS Discovery**
  - Works quite well in mobile networks
  - Real challenge in fixed networks due to RFC1918 and DNS forwarders on CPE/Home Gateway
    - Private address for local DNS proxy, DNS discovery via DDR fails
    - Requires software changes and might require changes how DNS is operated
    - Open market for Home Gateways, no (easy) update/upgrade possible

- **Impact of Encrypted Client Hello**
  - Uses encrypted DNS, what happens in case encrypted DNS not available (specifically in fixed network) due to non-working discovery?
  - Risk, that high number of DNS requests is moving away from ISPs DNS platform towards public resolvers


DNS Server
Encrypted DNS (www.example.com)
TLS1.3 Encrypted Client Hello
SNI(www.example.com)
WEB Server
Client