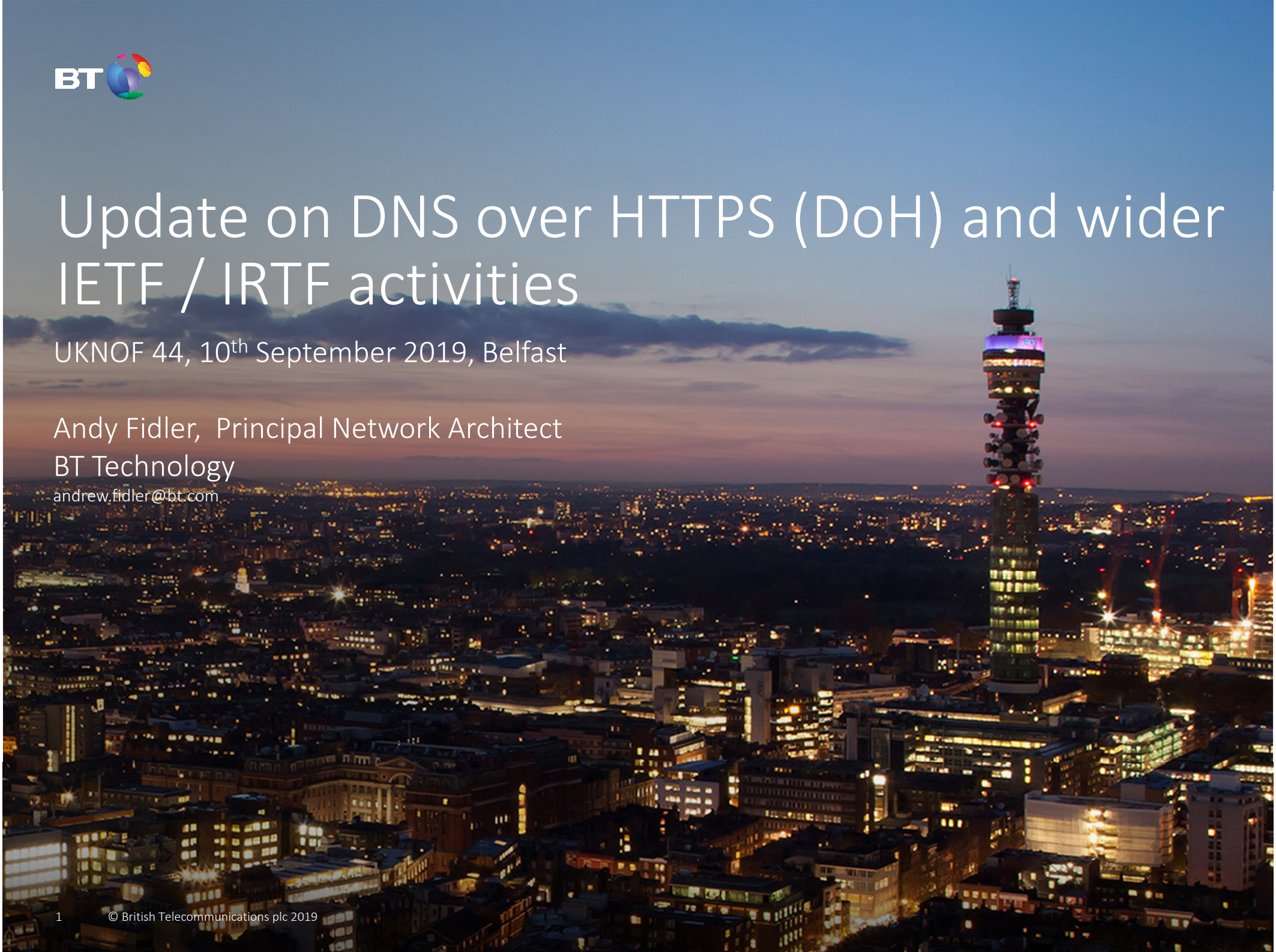


Update on DNS over HTTPS (DoH) and wider IETF / IRTF activities

UKNOF 44, 10th September 2019, Belfast

Andy Fidler, Principal Network Architect
BT Technology
andrew.fidler@bt.com

An update on the DoH of today, tomorrow and wider IETF activities

- **At UKNOF 43 we outlined the opportunities and risks created by DoH for ISPs and called for collaboration to address unintended consequences.**
  - https://indico.uknof.org.uk/event/46/contributions/668/attachments/898/1109/UKNOF43_Potential_ISP_challenges_with_DNS_over_HTTPS_Issue_1A_050419.pdf
- **Ecosystem discussions have evolved considerably since then.**
- **So today's presentation will start with an update on DoH, covering:**
  - **Latest Internet Engineering Task Force (IETF) DoH discussions, including IETF 105 Montreal take-outs**
  - **Browser and Operating System activities**
  - **Wider industry alliance and research activities**
  - **BT's position on DNS landscape and NXDOMAIN redirection**
  - **An overview of BT's DoH proof of concept and DNS roadmap**
- **Then moving onto the evolution of DoH from handful of browsers today, to mid-term 100s of applications and long term millions of IoT devices.**
- **And concluding with the question - is DoH just the tip of the iceberg of emerging IETF / IRTF activities that Operators need to analyse. Highlighting ESNI, QUIC and TLS 1.3 as examples.**

DoH Internet Engineering Task Force (IETF) Update

- **IETF 105 – Applications Doing DNS (ADD) Birds of Feather (BoF) session -** https://www.youtube.com/watch?v=n5UjPQksHT8
  - **Mozilla outlined their vision for DNS & apps**
  - **Google shared their perspective on DoH and DoH preference hints for HTTP**
  - **BT highlighted the need for DoH Best Current Practice guidelines**
  - **Jim Reid presented on non-browser apps doing DNS and DoH push**
  - **Mixed opinions expressed ranging from supporting calls for further best practice guidelines to view that DoH protocol work is complete**.

- **Next-steps steer from IETF Internet Engineering Steering Group (IESG) / Internet Architecture Board (IAB) meeting (week ending 23/8)** https://mailarchive.ietf.org/arch/msg/add/speQ9z679B21dZ3qBc6kT2-pYn4 **:**
  - **Agreement that there is work to do on DoH and that it is important to get it going sooner, rather than later.**
  - **Still reviewing how this work will be undertaken, e.g. via chartered items into an existing or new working group.**
  - **Also exploring possibility of a workshop to allow IETF community to undertake a focussed review of work requirements.**

- **Plus debates continue on the ADD mailing list -** https://www.ietf.org/mailman/listinfo/add

- **Cross eco-system engagement welcomed in updating previous DoH Internet-Drafts and/or creating new Best Current Practice guidelines.**

- **Also let's start planning now for discussions at IETF 106 – 16-22nd November, Singapore**
  https://www.ietf.org/how/meetings/106/

Browser / OS DoH status update

Mozilla / Firefox:

- **Capability to opt-in/select a DoH resolver exists in current live version.**
- **Mozilla have run studies to detect DNS-based parental controls and split-horizon aspects [1].**
- **Plan to gradually roll out DoH in the USA starting in late September [2].**
- **Presently have no plans to enable DoH by default in the UK.**

Google / Chrome:

- **Experimenting with DoH in Chrome 78 – branch cut 5/9, stable 22/10 (estimate), followed by launch if everything goes well [3].**
- **Intending to only enable DoH if users existing DNS resolver supports DoH.**
- **Will have a small table to map non-DoH servers to their equivalent DoH servers.**

Apple (iOS/macOS):

- **No native support for DoH currently**
- **Apple engineers at IETF are working on a solution to add DoH support at an operating system level**
- **Goals are to consider policy from users, enterprises, and local network admins; such as ISP/enterprise settings and captive portals.**

Microsoft:

- **Exploring with major browsers and ISPs interaction options between OS and Browser DNS settings.**

- **Key Take-out:**
  - **In the short-term, current browser DoH enablement plans should not significantly impact existing UK ISP services.**
  - **But Operators still need to plan for longer-term impacts which could be more significant as previously highlighted.**

[1] https://blog.mozilla.org/futurereleases/2019/07/31/dns-over-https-doh-update-detecting-managed-networks-and-user-choice/4
[2] https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/
[3] https://groups.google.com/a/chromium.org/forum/#!msg/net-dev/BgLpAi9O4MY/1i6UtqXTDgAJ

BT

Wider Industry DoH update

Comcast have launched an Encrypted DNS Deployment Initiative (EDDI)

- Goal of ensuring the smooth global deployment and reliable operation at scale of DNS encryption technology.
- It would be great to see cross ecosystem participation – browsers, applications, OS, ISPs/operators, DNS vendors, CDN vendors, etc.
- https://encrypted-dns.org and subscribe at https://lists.encrypted-dns.org

Various performance studies published suggesting no significant performance gap between DoH and plaintext DNS (Do53) https://samknows.com/blog/dns-over-https-performance & https://arxiv.org/abs/1907.08089

- SK study calls out impact of EDNS Client Subnet (ECS) blocking on certain ISP caches, solutions are still required for this issue.

In July – first examples of Malware using DoH to secure its communication channels – New Godlua Malware

- https://www.bleepingcomputer.com/news/security/new-godlua-malware-evades-traffic-monitoring-via-dns-over-https/

- A number of the smaller UK ISPs enable DoH resolvers
  - Given the enhanced profile of DoH in recent months, a number of the smaller UK ISPs / hosting providers have launched DoH.

Internet Service Provider Association (ISPA) UK held a July DoH workshop with attendees from ISPs, DNS vendors and UK Government / Regulators.

- A follow-on workshop may be organised for mid October.

European Telecommunications Network Operators (ETNO) Association are currently drafting up a position paper on DoH.

BT Broadband approach to DNS

- **BT position on DoH remains that we look favourably upon anything that improves privacy and security for our customers. However DoH may create ISP implementation issues and unintended consequences across the ecosystem. BT welcomes industry collaboration to develop solutions for these potential issues.**

- **BT has started a DoH Proof of Concept activity, which will focus on our BT Broadband capabilities.**

- **On NXDOMAIN redirection, BT Broadband intends to withdraw our current Web Address Help capability. Customers of 2020 require less help than those in 2010 when it was launched. Withdrawing this capability will also assist any subsequent roadmap enablement of DNSSEC.**

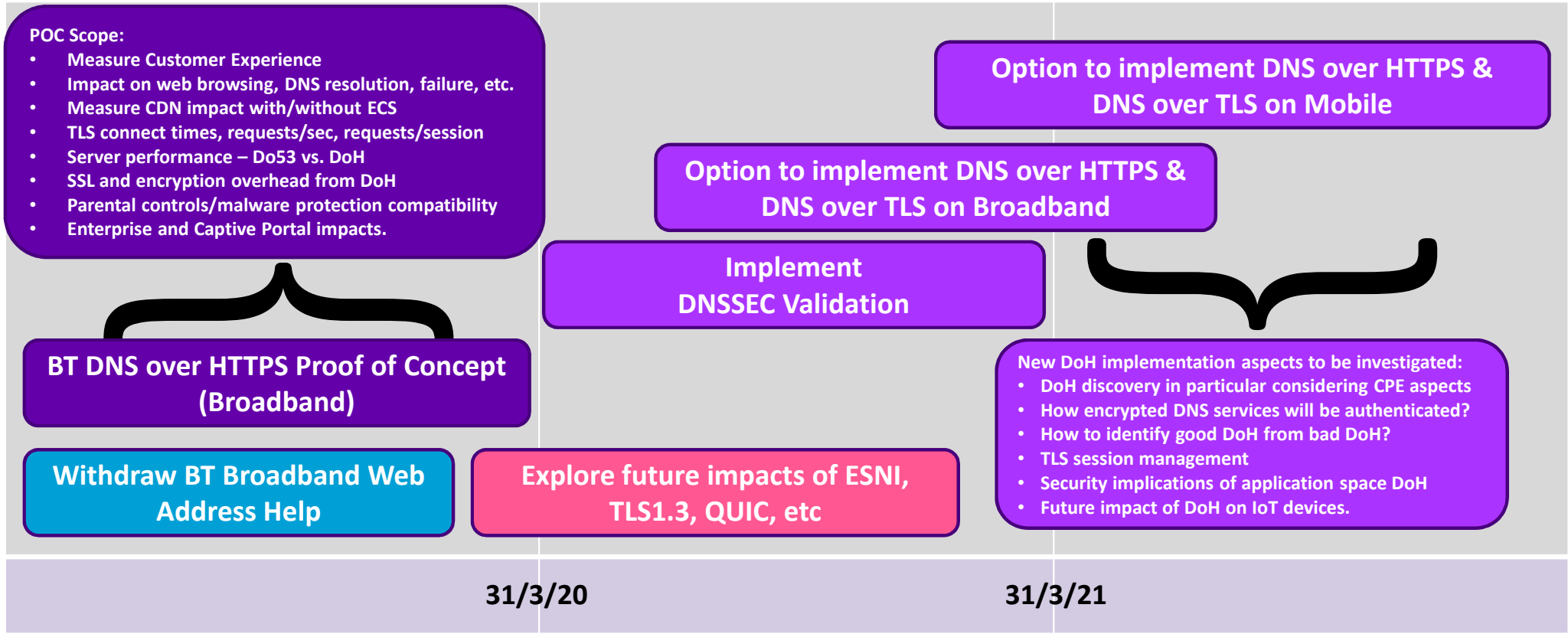
- **On CPE DNS options, historically BT Broadband hubs do not allow customers to change DNS settings to minimise complexity. This does not stop users selecting 3rd party DNS resolvers via device OS configurations.**

- **BT Broadband hubs do not do HTTPS interception or 'man-in-the-middle'. BT Broadband hubs only present a self-signed certificate for admin user interface connections.**

- **BT Broadband customers can opt-in to Parental Controls and select which content categories they would like to restrict access to. Our solution uses DNS-based content filtering. For HTTP traffic going to restricted categories, customers are presented with a redirect page explaining why the content is restricted and providing further options. For HTTPS traffic the content is restricted but we are unable to present a redirect page as this would look like a 'man-in-the-middle', hence some browsers may display a TLS error page. We also offer a DNS based malware protection capability.**

- **BT Broadband implements the UK Internet Watch Foundation (IWF) block list, which can only be applied to HTTP.**

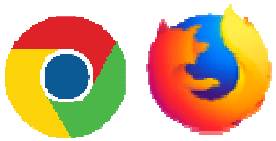
Indicative BT DNS roadmap



Note: Roadmap is for information / indicative purposes only and does not reflect any committed service capabilities / upgrades.

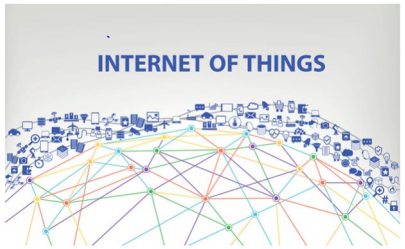
DoH – it's not just about browsers, what about mobile apps & IoT?

Evolution of DoH:



Current focus on Browsers

Future focus on Mobile Applications

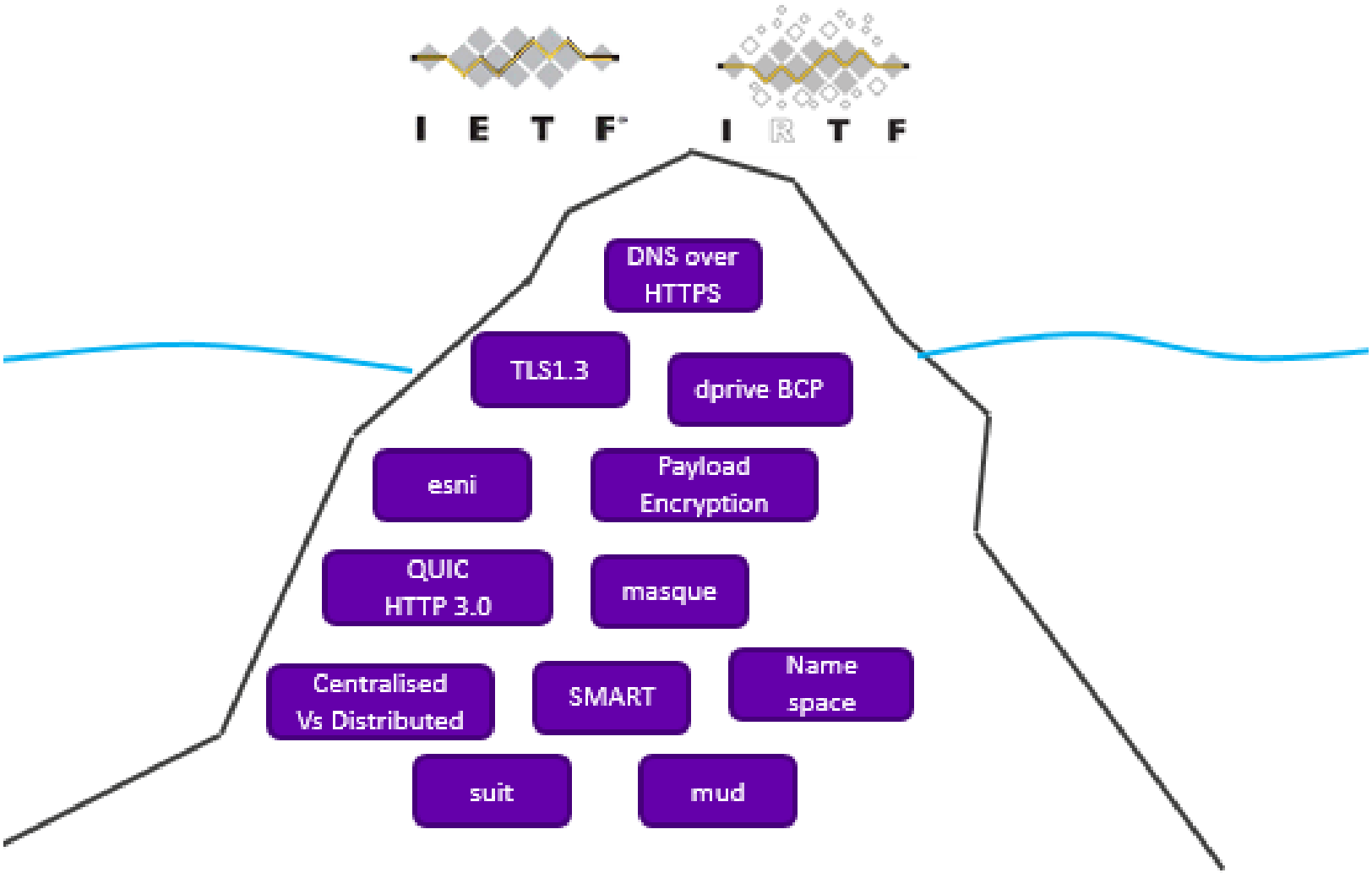


& IoT, e.g. Smart Homes

Unintended consequences of Mobile Apps & IoT?
Potentially opening up new malware risks for IoT devices?

Can IETF SUIT and MUD working groups assist here?
Software Update for Internet of Things (SUIT)
https://datatracker.ietf.org/doc/draft-ietf-suit-architecture/
Manufacturer Usage Description Specification (MUD)
https://datatracker.ietf.org/doc/rfc8520/
Alongside IoT Security Foundation (IOTSF) Guidelines
https://www.iotsecurityfoundation.org/best-practice-guidelines/

Is DoH just the tip of the iceberg of wider IETF / IRTF activities that need ISP/Operator analysis and engagement?

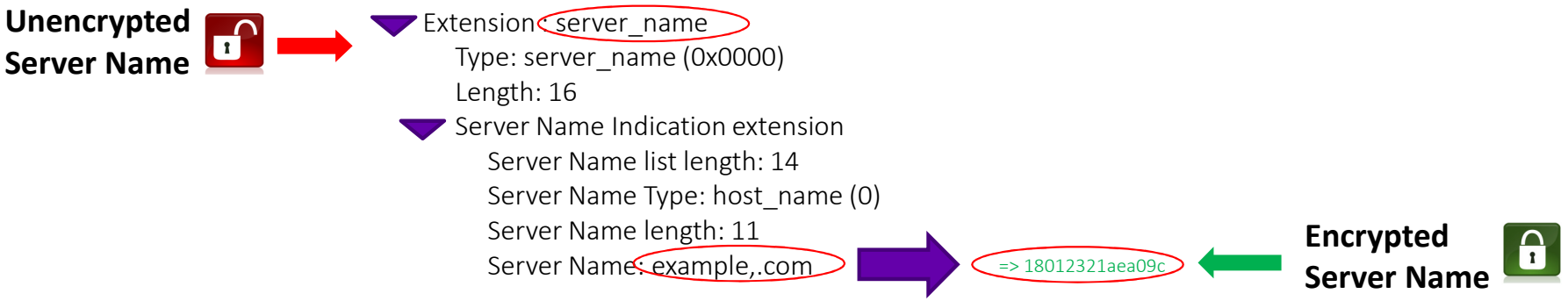


DNS Privacy Recommendations & Encrypted Service Name Indication

- **DNS Privacy:**
  - **IETF DNS PRIVate Exchange (dpriv) Working Group are drafting Best Current Practice Privacy recommendations for DNS Operators [1].**
  - **This may encourage more detailed benchmarking of DNS resolvers and DNSPrivacy.org are already looking at this [2].**
  - **We recommend ISPs review current drafts and consider alignment with recommended best practice.**

DNS Resolver	IP address logging	Data retention policy	Share anonymised data with partners	Share identifiable data with partners	Cyber security analysis	Combine DNS data with other sources	Redirect NXDOMAIN	DNS content blocking e.g. malware, parental controls	Support for DNSSEC, DoT & DoH	EDNS0 / ECS approach	Query Name Minimisation	DNS Response time	DNS failure rate, availability stats, etc.
A													

- **Encrypted Server Name Indication (ESNI):**
  - **Currently Server Name Indication (SNI) is passed in the clear within the Transport Layer Security (TLS) handshake**
  - **ESNI is a draft RFC proposing to encrypt this information, thus concealing the requested hostname [3].**
  - **Whilst enhancing privacy, this may also impact ISP use of SNI information, e.g. Zero Rating, Content Control**

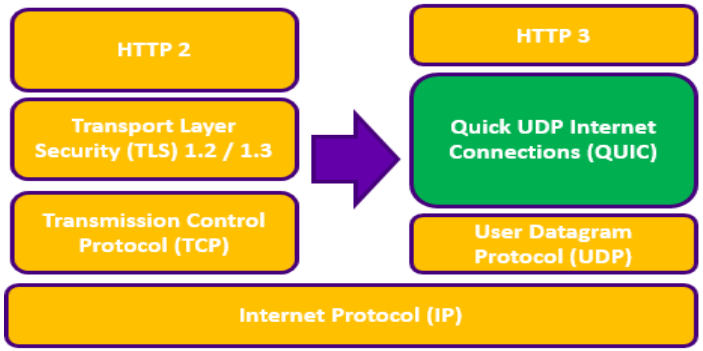


[1] https://datatracker.ietf.org/doc/draft-ietf-dprive-bcp-op/
[2] https://dnsprivacy.org/jenkins/job/dnsprivacy-monitoring/
[3] https://datatracker.ietf.org/doc/draft-ietf-tls-esni/

Transport Layer Security 1.3 & QUIC

- **Transport Layer Security (TLS) 1.3:**
  - **New version of TLS used to secure sessions between applications and servers – TLS 1.3 – RFC8446 [1]**
  - **Speeds up encrypted connections, removes obsolete/insecure features from TLS1.2 and encrypts more of the handshake, e.g. Certificate Name.**
  - **Standard is complete, but is the full impact of this understood?**
  - **Great from privacy perspective but creates deployment challenges, e.g. CPE upgrades, limitations for firewalls, proxies, middleboxes and session resumption requirements.**
  - **Also when TLS1.3 certs are combined with DoH & ESNI – maximises privacy for end-user but makes cyber-security threat detection harder.**

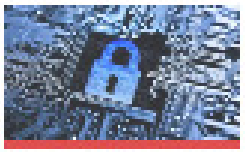
- **"Quick UDP Internet Connections" (QUIC):**
  - **A new UDP based multiplexed and secure transport protocol, with aim of HTTP3 over QUIC replacing existing HTTP over TCP & TLS 1.2 [2]**
  - **More efficient protocol by integrating security directly into transport and use of single round trip handshakes. Plus support for multiplexing & changing IP addresses.**
  - **Points for ISP consideration are opportunities for TV / content delivery, CPE support, multipath access capabilities and DNS over QUIC.**
  - **Operators may also want to consider wider aspects around payload and pervasive encryption [3].**



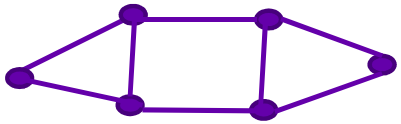
[1] https://tools.ietf.org/html/rfc8446
[2] https://datatracker.ietf.org/doc/draft-ietf-quic-transport/
[3] https://tools.ietf.org/html/draft-ietf-quic-manageability-05

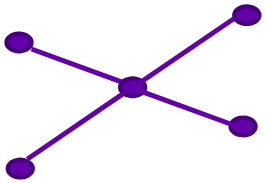
SMART & Consolidation of Internet Architecture

- **Stopping Malware and Researching Threats (SMART):**
  - **Informal Research Group exploring effects of existing, proposed and newly published protocols and internet standards on attack defence.**
  - **Gathering evidence from security practitioners and then making this available to protocol designers, implementers and users.**
  - **Encourage Operators, Vendors and Cyber-security researchers to get involved with the research and writing of new IETF Internet-Drafts.**
  - **See https://github.com/smart-rg/drafts/blob/master/draft-charter.md and https://github.com/smart-rg/drafts for more details**



- **Consolidation of Internet Architecture – Distributed vs Centralised:**
  - **Internet originally architected as the ultimate distributed platform**
  - **However as it has matured, we are seeing the growth of large centralised entities in many areas.**
  - **Debates ongoing within the IETF on Distributed vs Centralised**
  - **Encourage ISPs to engage in these discussions**
  - **See https://tools.ietf.org/html/draft-arkko-iab-internet-consolidation-01 & https://www.ietf.org/blog/consolidation/ for more details.**

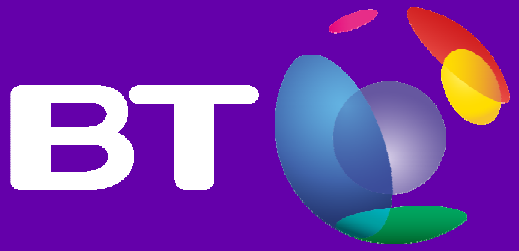




BT

Conclusion

- In conclusion:
  - We welcome the adoption of DNS Encryption (both DoT and DoH) to improve security for customers.
  - ISP implementation issues remain and we look to the IETF, industry alliances and wider ecosystem to address these through collaboration.
  - We see the newly formed Encrypted DNS Deployment Initiative playing a key role in these discussions.
  - BT has started a DoH proof of concept and is looking to roadmap DNSSEC, DoT and DoH opportunities for 20/21 and 21/22.
  - Browser implementation of DoH is just the starting point, industry needs to quickly assess the impact to mobile applications and IoT devices.
  - DoH is just the tip of the iceberg of IETF / IRTF activities that would benefit from ISP engagement and analysis.
  - We encourage operators to assess the opportunities, risks and unintended consequences that may be created by TLS 1.3, ESNI, QUIC, etc.
  - ….then directly engage in IETF and IRTF working groups as appropriate.


BT