EDDI 9.19.19 meetup

Legal Notices

Anti-Trust Guidelines for the Encrypted DNS Deployment Initiative

As with other initiatives to implement protocols across the Internet, the Encrypted DNS Deployment Initiative ("EDDI") seeks to ensure the smooth global deployment and reliable operation at scale of DNS encryption technology in an open and transparent way across the Internet. This effort necessarily involves global coordination across a wide range of technical actors, from protocol designers to software developers, network operators, DNS operators, content delivery networks, cloud providers, application providers, and many others. In order to advance the pro-competitive and pro-consumer objectives of EDDI, it is imperative that all participants in EDDI abide by the antitrust laws. While not exhaustive, the following guidelines are intended to aid in your compliance with the antitrust laws.

Participants in EDDI should consult with their own legal counsel on participation in the initiative and complying with all applicable laws.

1. Don't discuss competitively sensitive information, such as pricing, competitive strategy, and future product roadmaps. EDDI participants should not discuss with each other pricing, competitive strategy, future product roadmaps or other similar information that could be considered competitively sensitive.
2. Don't discuss with other participants in EDDI any joint action directed against another company, such as jointly refusing to deal with that other company.
3. Don't discuss with other participants in EDDI your confidential dealings with business partners, suppliers or vendors.
4. Don't discuss limiting competition or excluding competitors.
5. Don't use exaggerated language. EDDI is a forum to share best practices, information on deployment and technical trials, lessons learned, and efforts to measure, test, and implement DNS encryption at scale across the Internet ecosystem. All communications in any form should be focused on those efforts. EDDI participants should avoid the use of exaggerated language. You should assume that communications made through EDDI are not confidential and will be shared outside of EDDI.

These guidelines are not intended to be exhaustive of the types of activities that are and are not appropriate for EDDI participants. If you have any questions about the application of these guidelines to particular facts and circumstances or questions regarding complying with the antitrust laws, please consult your own legal counsel.

Agenda

- Welcome & Introductions
- What EDDI isn't
- Workstream ideas
- How to work together
- EDDI Outreach
- Next Steps

Agenda

- Welcome & Introductions
- What EDDI isn't
- Workstream ideas
- How to work together
- EDDI Outreach
- Next Steps

Agenda

- Welcome & Introductions
- What EDDI isn't
- Workstream ideas
- How to work together
- EDDI Outreach
- Next Steps

Agenda

- Welcome & Introductions
- What EDDI isn't
- Workstream ideas
- How to work together
- EDDI Outreach
- Next Steps

Workstreams
Brainstorming possible workstreams

Testing & Measurement
Would be nice to have a standard recommended dnsperf test configuration, so across different implementers there is an apples-to-apples benchmark tool - https://www.dnsperf.com/
This can also be used by independent measurement researcher & orgs

Resolver Discovery & Selection
Needs to handle one or more FORWARDERS between client and full resolver
If done right, will provide *DNS Traceroute* functionality, at last
Overlapping RFC-1918 scopes may result in forwarders and/or the final resolver not being directly accessible from the client
Forwarders and resolvers might not have public FQDNs and may not even have private FQDNs
Need some unique name in an available namespace that is guaranteed to not collide
Maybe base on IPv6 ULA or some other GUID name-generator

Canary Domains / Conflict Detection
Should only be local and should be relative to server's locally scoped name (if that is even possible)
E.g. canary-domain.forwarder-or-resolver-name.local (not literally, just semantically)

Workstreams
Brainstorming possible workstreams

Scaling / Architecture Discussions
Support for forwarding may be necessary to maintain parity with current scaling (e.g. ratios)
New DNS flag or EDNS flag or OPT to signal request to encrypt (including propagation of flag and encryption)
May require new kind of flag or OPT that is NOT hop-by-hop, but rather is propagated to from the originating client to the full resolver
See "Recursive-to-Authoritative" below as well

Security / Attack Resilience
Downgrade resistance is necessary
DNSSEC signing is very likely a requirement regardless of specific mechanism(s)
DANE TLSA records should probably be mandatory unless someone can provide counter-examples

DoT Positioning
Propose that DoH exclusive of DoT is not acceptable to the DNS community at large
Propose that resolver choices need to include DoT-only providers, and that DoH vs DoT needs to be exposed to users if a provider supports both
Propose DoT blocking be used as a proxy signal for network policy (substitute for canary domains)

Workstreams
Brainstorming possible workstreams

DNS Data Policies
Best practices concerning logging, use, disclosure, etc.

Opt-in vs opt-out
Generally, opt-out is a terrible idea, something that has been demonstrated repeatedly.

RPZ and Trust Anchor Issues
Trust anchor(s), provisioning/publishing of such, maybe via resolver-naming authoritative RRs? Self-signed or not?
Use trust anchors to auto-discover split-DNS environment (resolver type)?
Use trust anchors to auto-discover RPZ servers (or combined RPZ server-resolvers)?
Order trust anchors to prevent abuse or to scope functionality (no squatting, maybe private domains and/or RPZ only), including RPZ-first vs RPZ-second (no-cache vs cache)
Signing RPZ-specific responses?
Changes to RPZ architecture to allow mixing RPZ and non-RPZ resolvers?
Add structure to current unordered "nameserver" list in /etc/resolv.conf, similar to SRV semantic mechanisms?

Workstreams
Brainstorming possible workstreams

Recursive-to-Authoritative
Encryption generally is okay, but simply replacing Do53 with ADoT (for example) causes immediate scaling pain
"Poster child" of scaling: large recursive operator (google or cloudflare) to large authority operator (godaddy)
Site-to-site encryption mechanisms may scale better
Separate transport from DNS messages to facilitate scaling
Open question: is it desirable/necessary to facilitate anonymity of resolver operators, or would a mechanism that requires enrollment or coordination or identification be acceptable?

Things to document
DNS current uses and use cases so that proposals can be evaluated to score what works/what breaks
Capture any territorial compliance/legal requirements

Other Random Stuff
Develop short presentation that any participant can use to do a 5-minute lightning talk overview of EDDI at workshops/meetings/conferences

Agenda

- Welcome & Introductions
- What EDDI isn't
- Workstream ideas
- How to work together
- EDDI Outreach
- Next Steps

Agenda

- Welcome & Introductions
- What EDDI isn't
- Workstream ideas
- How to work together
- EDDI Outreach
- Next Steps

Agenda

- Welcome & Introductions
- What EDDI isn't
- Workstream ideas
- How to work together
- EDDI Outreach
- Next Steps

Links

EDDI

https://www.encrypted-dns.org/

Archive

http://lists.encrypted-dns.org/scripts/waENCDNS.exe?A0=ENCRYPTED-DNS

GitHub

https://github.com/Encrypted-DNS-Deployment-Initiative