Encrypted DNS
Deployment Initiative

EDDI@DNS-OARC32

in partnership with DNS-OARC & sponsored by Comcast

EDDI 2.9.20

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

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

Agenda

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

Agenda

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

EDDI Objective:

- The goal of the Encrypted DNS Deployment Initiative is to ensure the smooth global adoption and reliable operation at scale of DNS encryption technology. This effort involves global coordination across a wide range of technical professionals, from protocol designers to software developers, network operators of all types, DNS operators, content delivery networks, cloud providers, application providers, and many others.

EDDI will…

- *Strive to define and adopt DNS encryption technologies in a manner that ensures the continued high performance, resiliency, stability and security of the Internet's critical namespace and name resolution services, as well as ensuring the continued unimpaired functionality of security protections, parental controls, and other services that depend upon the DNS.*

- *Seek to enhance the privacy and security of users, devices and services through the encryption of DNS query and response traffic and other techniques for reducing the disclosure of potentially sensitive information in DNS traffic.*

- *Develop best practices, such as in areas that may explore the collection and use of data contained in DNS queries, resolver discovery and selection, and how end user configuration options may be presented.*

Approach…

Bring together key players in the implementation ecosystem

Provide a forum for discussing, sharing, and developing as necessary:

- Measurement data
- Design, deployment, and operations experience (e.g. lessons learned)
- Technical methods to address the needs of specific types of networks and service dependencies, including enterprise, government, and school networks, as well as ISP networks.
- Cyber-security and malware protections
- Parental content controls

How to Participate…

WWW.ENCRYPED-DNS.ORG

EDDI MAILING LIST

&

PUBLIC ARCHIVES

EDDI WORK STREAMS IN EDDI GITHUB REPOSITORIES

ATTEND EDDI MEETUPS

Agenda

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

Agenda

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

Agenda

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

Agenda

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

Agenda

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

Adaptive DNS Discovery (ADD) - Proposed Working Group Charter

Sending DNS messages over encrypted transports, as defined in DNS over TLS (DoT) [RFC 7858] and DNS over HTTPS (DoH) [RFC 8484], provides benefits to the security and privacy of DNS data. Clients, such as applications and host operating systems, have started adopting these protocols to provide these user benefits.

This working group will focus on discovery and selection of DNS resolvers by DNS clients in a variety of networking environments, including public networks, private networks, and VPNs, supporting both encrypted and unencrypted resolvers. It is chartered solely to develop technical mechanisms. Making any recommendations about specific policies for clients or servers is out of scope.

Clients adopting encrypted DNS protocols need to determine which DNS servers support those protocols, and which server to use for specific queries if multiple servers are available. These decisions can vary based on the network environment, and also based on the content and purpose of the client queries.

Network operators that start offering DNS encryption on their servers also need a way to indicate this support to clients. Communicating information about resolver configuration and behavior allows clients to make more informed decisions about which DNS servers to use. For example, a resolver may be able to resolve private or local names as a split DNS server.

Adaptive DNS Discovery (ADD) - Proposed Working Group Charter

The Adaptive DNS Discovery (ADD) working group will work on the following deliverables:

- Define a mechanism that allows clients to discover DNS resolvers that support encryption and that are available to the client either on the public Internet or on private or local networks.

- Define a mechanism that allows communication of DNS resolver information to clients for use in selection decisions. This could be part of the mechanism used for discovery, above.

- Develop an informational document that describes mechanisms for clients to detect specific network environments (such as captive portal and split horizon) and to use that information to inform their DNS configuration.

This working group will coordinate with dnsop, doh, and dprive for any changes required in DNS protocols and will make sure that those groups are included in major document reviews at appropriate times. It will also work with capport to ensure that solutions are applicable to captive networks.

Agenda

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

Use Cases

Several decades of creative operational uses of DNS need capturing

….contribute yours

GitHub:

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

Taxonomy:

../Use-Cases/blob/master/Taxonomy.md

Format:

Template based on RFC7744 to be posted in github repository

Agenda

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

Meetups

- London – March 2, 2020
- IETF107 Vancouver side meeting March 22-26
- IETF108 Madrid
- More to come in 2020

Past meetings & materials:
https://github.com/Encrypted-DNS-Deployment-Initiative/Reference

Agenda

9:00 Start :: 12:30 Finish

Part 1: 1.5 hrs 9:00-10:30

- Agenda Bash
- Introductions (15m)
- EDDI Overview – Glenn Deen (5m)
- Deployments (40m)
  - Erik Bishop Comcast (20m)
  - Nic Leymann DT (20m)
- Tommy Jenson Microsoft (30m)

Coffee Break (30min) 10:30-11:00

Part 2: 1.5 hrs 11:00-12:30

- IETF activity (40m)
- Use-Cases & Taxonomy (30m)
- Next steps & future meetups (20m)
- AOB (5)

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