

4 January 2021

RE: Comments on Mozilla's DoH and TRR

Mozilla Corporation  
331 East Evelyn Avenue  
Mountain View, CA 94041  
[REDACTED]

ICANN appreciates the opportunity to respond to Mozilla's request for comments on DNS-over-HTTPS (DoH) and Mozilla's trusted recursive resolver (TRR) program. Some stakeholders in ICANN's community are concerned with how Firefox's implementation of DoH, like any implementation of DoH, can potentially have an impact on the openness, interoperability, resilience, security, and/or stability of the DNS.

ICANN's view of encrypted DNS is given in OCTO-003, "Local and Internet Policy Implications of Encrypted DNS" <<https://www.icann.org/octo-003-en.pdf>>. That document (which is periodically updated) lists ICANN's four positions on encrypted DNS:

- Communication privacy is good;
- DNS filtering can be beneficial;
- Applications and operating systems have insufficient information; and
- DNS data should be protected.

In response to Mozilla's request for input on how to maximize the security benefits of Firefox's implementation of DoH, we strongly encourage Mozilla to add a requirement to the TRR program that all trusted resolvers must perform DNSSEC validation. DoH, in and of itself, protects the communication channel but does nothing to protect the resolver from cache poisoning. This additional protection is missing from the current TRR program, and its inclusion would lead to Firefox's users being protected from DNS data modification and thus, protected from well-known attacks on the resolvers to which they have been redirected.

Another important improvement that Mozilla could make pm the TRR program would be easier-to-find instructions for ISPs and enterprise resolver operators on how to prevent their customers from using Firefox's TRRs when those operators are offering important local services such as filtering.

We look forward to seeing how Mozilla improves its services based on this request for public comments.

Sincerely,



David Conrad, Chief Technical Officer  
ICANN