"Existing" solutions to DNS encryption - draft-bortzmeyer-dnsop-privacy-sol-00

Stéphane Bortzmeyer - AFNIC

IETF 89 - London

DTLS? RFC 6347

Pros:

1. TLS (lot of experience and code)
2. UDP-specific which is cool for DNS
3. Used in WebRTC
4. Implemented in OpenSSL

Cons:

1. DTLS requires prior association, so we no longer have a stateless request-response protocol. Scalability?

Do we need to write an I-D "How to use DTLS to protect DNS"? What needs to be specified? Any DTLS expert to help?
If endorsed by the IETF for DNS confidentiality, how to make it happen? What are the steps towards deployment?

DNScrypt/DNScurve

- DNScurve protects resolver $\leftrightarrow$ authserver. Key is found in the delegation.
- DNScrypt protects stub resolver $\leftrightarrow$ resolver. Key is manual.

Pros:

1. Already implemented

Cons:

1. Little deployment
2. Change control problems