The next step for DPRIVE

Stéphane Bortzmeyer - AFNIC

IETF 97 - Seoul
Current state

The next step for DPRIVE
Charter said “primary focus [...] to develop mechanisms that provide confidentiality between DNS Clients and Iterative Resolvers”
Charter said “primary focus [...] to develop mechanisms that provide confidentiality between DNS Clients and Iterative Resolvers”

RFC 7858 and draft-ietf-dprive-dtls-and-tls-profiles provides encryption and stub resolver authentication
Current state

- Charter said “primary focus [...] to develop mechanisms that provide confidentiality between DNS Clients and Iterative Resolvers”
- RFC 7858 and draft-ietf-dprive-dtls-and-tls-profiles provides encryption and stub resolver authentication
- Charter also says “may also later consider mechanisms that provide confidentiality between Iterative Resolvers and Authoritative Server”
Do not reinvent the wheel: reuse DNS-over-(D)TLS

This leaves the issue of authentication.

The next step for DPRIVE
Proposal

- Do not reinvent the wheel: reuse DNS-over-(D)TLS
Proposal

- Do not reinvent the wheel: reuse DNS-over-(D)TLS
- This leaves the issue of authentication
Big difference

Stub \rightarrow Resolver: few servers, static config such as key pinning is OK

Resolver \rightarrow Authoritative: many servers, need something more dynamic
Big difference

- stub → resolver: few servers, static config such as key pinning is OK

Stéphane Bortzmeyer - AFNIC  
The next step for DPRIVE
Big difference

- **stub** → **resolver**: few servers, static config such as key pinning is OK
- **resolver** → **authoritative**: many servers, need something more dynamic
Possible techniques of authentication

[Should be all in draft-bortzmeyer-dprive-step-2]
Possible techniques of authentication

[Should be all in draft-bortzmeyer-dprive-step-2]

- Encode key in name (DNScrypt-style)
Possible techniques of authentication

[Should be all in draft-bortzmeyer-dprive-step-2]

- Encode key in name (DNScrypt-style)
- Regular PKIX validation based on DNSname
Possible techniques of authentication

- Encode key in name (DNScrypt-style)
- Regular PKIX validation based on DNSname
- Key in DNS (DANE)
Possible techniques of authentication

[Should be all in draft-bortzmeyer-dprive-step-2]

- Encode key in name (DNSCrypt-style)
- Regular PKIX validation based on DNSname
- Key in DNS (DANE)
- ...
Possible techniques of authentication

[Should be all in draft-bortzmeyer-dprime-step-2]

- Encode key in name (DNScrypt-style)
- Regular PKIX validation based on DNSname
- Key in DNS (DANE)
- ...

Difficult balance between too few and too many choices. What to do if client wants DANE and server only has a PKIX cert?
Tasks

- Decide on one (or several) solutions in draft-bortzmeyer-dprive-step-2
- Write an I-D
- Do we need to update the charter?
Tasks

- Decide on one (or several) solutions in draft-bortzmeyer-dprive-step-2
Tasks

- Decide on one (or several) solutions in draft-bortzmeyer-dprise-step-2
- Write an I-D
Tasks

- Decide on one (or several) solutions in draft-bortzmeyer-dprive-step-2
- Write an I-D
- Do we need to update the charter?