Requirements for Privacy Services Between Recursive Resolvers and Authoritative Servers

Goals

- Begin developing consensus on requirements
- Identify missing requirements
- Identify unnecessary requirements

Process

- Open discussion of each identified requirement in the document
- Chairs/Authors prioritized order of requirements based on mailing list traffic
- Work through open questions & concerns with each requirement in Section 5.1
- Continue process via interims prior to IETF 110 (we won't finish all 11 today)
- All decisions will be confirmed on mailing list

Requirement 7

The authoritative domain owner or their administrator MUST have the option to specify their secure transport preferences (e.g. what specific protocols are supported). This SHALL include a method to publish a list of secure transport protocols (e.g. DoH, DoT and other future protocols not yet developed). In addition this SHALL include whether a secure transport protocol MUST always be used (non-downgradable) or whether a secure transport protocol MAY be used on an opportunistic (not strict) basis in recognition that some servers for a domain might use a secure transport protocol and others might not.

Requirement 2

A recursive resolver that supports recursive-to-authoritative DNS encryption MUST be able to determine whether or not a given authoritative name server to which it intends to connect also supports recursive-to-authoritative DNS encryption.

Requirement 3

An authoritative name server that supports recursive-to- authoritative DNS encryption MUST be able to indicate that it supports recursive-to-authoritative DNS encryption in a way that facilitates (2).

Requirement 9

A given name server may be authoritative for multiple zones. As such, a name server MAY support use of a secure transport protocol for one zone, but not for another.

Requirement 8

The authoritative domain owner or their administrator MUST have the option to vary their preferences on an authoritative nameserver to nameserver basis, due to the fact that administration of a particular DNS zone may be delegated to multiple parties (such as several CDNs), each of which may have different technical capabilities. This includes that some servers for a domain may use secure transport and others may not, as it is common for a given name server to be authoritative for multiple zones.

Requirement 6

Each implementing party MUST be able to negotiate use of a secure transport protocol or other DNS privacy protections in a manner that enables operators to perform appropriate performance and security monitoring, conduct relevant research, etc.

Requirement 10

The specification of secure transport preferences MUST be performed using the DNS and MUST NOT depend on non-DNS protocols.

Requirement 1

Each implementing party MUST be able to independently take incremental steps to meet requirements without the need for close coordination (e.g. loosely coupled).

Requirement 4

An authoritative name server that does not support recursive-to- authoritative MUST NOT have to make any changes to facilitate (2).

Requirement 5

The secure transport MUST only be established when referential integrity can be verified, MUST NOT have circular dependencies, and MUST be easily analyzed for diagnostic purposes.

Requirement 11

For secure transports using TLS, TLS 1.3 (or later versions) MUST be supported and downgrades from TLS 1.3 to prior versions MUST not occur.