Recursive to Authoritative DNS with Encryption

Peter van Dijk, Paul Hoffman

IETF 110 DPRIVE

March 2021

draft-ietf-dprive-opportunistic-adotq

Reminder

This draft is already part of the WG consensus process.

If you want changes, we will make them.

Terminology

ADo*	(resolver to) authoritative DNS over some secure transport
ADoTQ	draft-ietf-dprive-opportunistic-adotq
ADoX	draft-rescorla-dprive-adox
Do53	'classic' clear text DNS over UDP/TCP port 53
unauth	unauthenticated
auth	authenticated

Draft principle (unauthenticated case)

1. Client asks resolver (empty cache) for `www.example.com.`
2. Resolver goes to `.`, `com.`, eventually learns:
   - `example.com. IN NS ns1.example.com.`
   - `example.com. IN NS ns2.example.com.`
3. Resolver asks `www.example.com.` over 'normal' Do53.
4. Resolver responds to client, client is no longer waiting.
5. Resolver now goes and learns that these name servers support DoT.
6. Resolver remembers this for later.
7. Next client asks for `mail.example.com.`
8. Resolver does this query over DoT.

Draft history

1st version

Real RFC 7435 opportunistic only. The discovery mechanism was 'probe the DoT port'.

→ WG desired (compatibility with) fully-authenticated but no such draft was present yet.

2nd version

We added a skeleton of fully-authenticated operation, and downgraded the opportunistic method to unauthenticated behaviour. Discovery mechanism is `TLSA`.

and then

.. a fully-authenticated pre-draft appeared! (Discovery mechanism: `SVCB`). Drafts overlap/conflict now. 3rd version will certainly be different (smaller?) again.

Service Discovery

ADoTQ unauth	TLSA on NS name
ADoTQ auth	TLSA on NS name
ADoX	SVCB in parent (Additional section) and/or SVCB on NS name

Changing to ADoX's use of SVCB makes sense for ADoTQ's service discovery.

Supported transports

ADoTQ unauth	DoT, DoQ
ADoTQ auth	DoT, DoQ
ADoX	DoT, DoQ, DoH

Changing to ADoX's use of SVCB makes sense in case the WG wants to support DoH.

Authenticating the server

ADoTQ unauth	Irrelevant
ADoTQ auth	TLSA from service discovery
ADoX	• WebPKI • maybe TLSA from an additional DNS request • TLS handshake (tls-dnssec-chain-extension)

Resolution if no service is found in cache for a zone's name servers

ADoTQ unauth	Use classic, then lookup
ADoTQ auth	Have to lookup first
ADoX	Lookup first

Resolution if service is discovered for a zone's name servers

ADoTQ unauth	Try every discovered server until one completes.
	↳ If none complete, fall back to classic DNS
ADoTQ auth	Try every discovered server until one completes
	↳ If none complete, send SERVFAIL
ADoX	SHOULD try all
	↳ [[OPEN ISSUE: figure out error details]]

Failure to authenticate the server

ADoTQ unauth	Ignore failures
ADoTQ auth	Fail connection
ADoX	Fail connection

Maybe the WG wants to move ADoTQ auth specification to ADoX document?

Next steps

- Document was purely RFC 7435 opportunistic at first.
- WG appeared to desire combining or at least syncing use cases.
- No authenticated document was submitted at the time.
- Now ADoX is under active consideration.
- Happy to remove all auth from this document and keep the discovery, if the WG wants.
- Or spin off discovery into a third (to then become first) draft for ADoTQ and ADoX to both refer to.