

DNS over CoAP – Updates

`draft-ietf-core-dns-over-coap`

Martine S. Lenders (martine.lenders@tu-dresden.de), Christian Amsüss, Cenk Gündoğan

Thomas C. Schmidt, Matthias Wählisch

IETF CoRE WG Interim Meeting, 2025-02-12

Reference in **8. Security Considerations** updated to draft rather than PR

General CoAP security considerations in Section 11 of [RFC7252] apply to DoC. Additionally, DoC uses request patterns that require the maintenance of long-lived security contexts. Section 2.6 of [I-D.ietf-core-corr-clar] goes into more detail on what needs to be done when those are resumed from a new endpoint.

Added to 4.3. DNS Responses in CoAP Responses

4.3.3. DNS Update

Until future work provides considerations for DNS Update [RFC2136], a DoC server that receives a query with the UPDATE opcode SHOULD indicate in its response that it does not implement DNS Update, see [RFC2136].

Amended notes on encryption and DNSSEC to 8. Security Considerations

A user of DoC must be aware that the DoC server may communicate unencrypted with the upstream DNS infrastructure, e.g., using DNS over UDP. DoC can only guarantee confidential communication and integrity between parties for which the security context is exchanged. The DoC server may use another security context to communicate confidentially and with integrity upstream (e.g., DNS over QUIC [RFC9250]) or just integrity (e.g., DNSSEC [RFC9364]), but, while recommended, this is opaque to the DoC client on the protocol level.

A DoC client may not be able to perform DNSSEC validation, e.g., due to code size constraints, or due to size of the responses. It may trust its DoC server to perform DNSSEC validation; how that trust is expressed is out of scope of this document. A DoC client may be, for instance, configured to use a particular credential by which it recognizes an eligible DoC server. That information can also imply trust in the DNSSEC validation by that server.