Constrained RESTful Environments
Internet-Draft
Intended status: Informational
Expires: 8 January 2026

M. S. Lenders
TU Dresden
C. Amsüss
T. C. Schmidt
HAW Hamburg
M. Wählisch
TU Dresden & Barkhausen Institut

7 July 2025

Discovery of Network-designated OSCORE-based Resolvers: Problem Statement
draft-lenders-core-dnr-06

Abstract

This document states problems when designing DNS SVCB records to discover endpoints that communicate over Object Security for Constrained RESTful Environments (OSCORE) [RFC8613]. As a consequence of learning about OSCORE, this discovery will allow a host to learn both CoAP servers and DNS over CoAP resolvers that use OSCORE to encrypt messages and Ephemeral Diffie-Hellman Over COSE (EDHOC) [RFC9528] for key exchange. Challenges arise because SVCB records are not meant to be used to exchange security contexts, which is required in OSCORE scenarios.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://netd-tud.github.io/draft-lenders-core-oscore-svcb/draft-lenders-core-dnr.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-lenders-core-dnr/.

Discussion of this document takes place on the Constrained RESTful Environments Working Group mailing list (mailto:core@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/core/. Subscribe at https://www.ietf.org/mailman/listinfo/core/.

Source for this draft and an issue tracker can be found at https://github.com/netd-tud/draft-lenders-core-oscore-svcb.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 8 January 2026.

Copyright Notice

Table of Contents

1. Introduction

The discovery of Internet services can be facilitated by the Domain Name System (DNS). To discover services of the constrained Internet of Things (IoT) using the DNS, two challenges must be solved. First, the discovery of a DNS resolver that supports DNS resolution based on secure, IoT-friendly protocols宴俳therwise the subsequent discovery of IoT-tailored services would be limited to resolution protocols conflicting with constrained resources. Second, the discovery of an IoT-friendly service beyond the DNS resolution.

[RFC9460] specifies the "SVCB" ("Service Binding") DNS resource record to lookup information needed to connect to a network service. Service Parameters (SvcParams) carry that information within the SVCB record.

The discovery of recursive DNS resolvers can be enabled by the DNS itself [RFC9461], [RFC9462] or, in a local network, by Router Advertisements and DHCP [RFC9463]. In all theses cases, the SvcParams is used, but supports only DNS transfer based on Transport Layer Security (TLS), namely DNS over TLS (DoT) [RFC7858], DNS over HTTPS (DoH) [RFC8484], and DNS over Dedicated QUIC (DoQ) [RFC9250]. The use of DoT, DoH, or DoQ, however, is not recommended in IoT scenarios.

DNS over CoAP [I-D.ietf-core-dns-over-coap] provides a solution for encrypted DNS in constrained environments. The Constrained Application Protocol (CoAP) [RFC7252] is mostly agnostic to the transport layer CoAP can be transported over UDP, TCP, or WebSockets [RFC8323], and even less common transports such as Bluetooth GATT [I-D.amsuess-core-coap-over-gatt] or SMS [lwm2m] are discussed. [I-D.ietf-core-transport-indication] covers the selection of different CoAP transports using SVCB records.

CoAP offers three ways of secure communication:

* *No Security:* This plain CoAP mode does not support any encryption (NoSec in Section 9 of [RFC7252]). It is not recommended when using [I-D.ietf-core-dns-over-coap] but inherits core CoAP features such as block-wise transfer [RFC7959] for datagram-based segmentation. Such features are beneficial in constrained settings even without encryption.

* *Transport Security:* CoAP may use DTLS when transferred over UDP [RFC7252] and TLS when transferred over TCP [RFC8323].

* *Object Security:* Securing content objects can be achieved using OSCORE [RFC8613]. OSCORE can be used either as an alternative or in addition to transport security.

  OSCORE keys have a limited lifetime and need to be set up. Keys can be established through an EDHOC key exchange [RFC9528], received from an ACE Authorization Server (AS, as described in the ACE OSCORE profile [RFC9203]), or through a combination of those (established with an EDHOC peer whose public key is confirmed by an AS, using the ACE EDHOC profile [I-D.ietf-ace-edhoc-oscore-profile]).

The SVCB-based discovery of CoAP services with no security and transport security is covered in [I-D.ietf-core-transport-indication]. The discovery of CoAP services, however, with object security is not specified. To guide future specifications, this document clarifies aspects when using SVCB in the context of CoAP and object security.

2. Terminology

The terms "DoC server" and "DoC client" are used as defined in [I-D.ietf-core-dns-over-coap].

The terms "constrained node" and "constrained network" are used as defined in [RFC7228].

SvcParams denotes the field in either DNS SVCB/HTTPS records as defined in [RFC9460], or DHCP and RA messages as defined in [RFC9463]. SvcParamKeys are used as defined in [RFC9460].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Problem Space

The first and most important point of discussion for the discoverability of CoAP is if and what new SvcParamKeys need to be defined and what is already there.

[RFC9460] defines the "alpn" key, which is used to identify the protocol suite of a service binding using its Application-Layer Protocol Negotiation (ALPN) ID [RFC7301]. While this is useful to identify classic transport layer security, the question is raised if this is needed or even helpful for when there is only object

security. There is an ALPN ID for CoAP over TLS that is defined in [RFC8323]. As using the same ALPN ID for different transport layers is not recommended, another ALPN ID for CoAP over DTLS is introduced in [I-D.ietf-core-coap-dtls-alpn]. Object security may be selected in addition to transport layer security or without it. Additionally, different CoAP transports can be selected, which may be orthogonal to the transport security. For instance, DTLS can be used over transports other than UDP. The selection of CoAP transport protocols will be covered in future versions of [I-D.ietf-core-transport-indication]. Defining an ALPN ID for each combination of object security, mode of transport layer security, and transport protocol might not be viable or scalable. For some ways of setting up object security, additional information is needed, such as an establishment options for an encryption context with EDHOC or an authentication server (AS) with ACE.

Beyond the SvcParamKeys, there is the question of what the field values of the Encrypted DNS Options defined in [RFC9463] might be with EDHOC or ACE EDHOC. While most fields map, "authentication-domain-name" (ADN) and its corresponding ADN length field may not matter when authentication is driven by Authorization for Constrained Environments (ACE) [RFC9203] [I-D.ietf-ace-edhoc-oscore-profile].

4. Objectives

SVCB records are not meant and should not be used to exchange security contexts, so this eliminates scenarios that use pre-shared keys with OSCORE. This leaves 2 base scenarios for OSCORE, which may occur in combination, with scenarios using transport security, or alternative transport protocols:

* DoC over OSCORE using EDHOC, and

* DoC using any ACE profile that eventually produces an OSCORE context.

We mostly need to answer the question for additional SvcParamKeys. [RFC9460] defines the keys "mandatory", "alpn", "no-default-alpn", "port", "ipv4hint", and "ipv6hint". Additionally, [I-D.ietf-core-dns-over-coap] defines "docpath" which carries the path for the DNS resource at the DoC server as a CBOR sequence.

Since "alpn" is needed for transport layer security, the type of object security (OSCORE using EDHOC, OSCORE using ACE, OSCORE using EDHOC using ACE), needs to be conveyed in a different SvcParamKey. The semantics and necessacity of the authenticator-domain-name field in [RFC9463] needs to be evaluated in each case.

When using ACE, more SvcParamKeys might be needed, such as the OAuth audience, the scope or the authentication server URI.

Defining these SvcParamKeys, including their value formats and spaces, as well as the behavior definition for the authenticator-domain-name field, shall be part of future work.

4.1. Scenarios

Two example scenarios illustrate possible ways for which a solution should work; they are phrased in dialogue form rather than in terms of protocol elements to avoid bias on solutions.

4.1.1. Neighbor discovered server with EDHOC credential

In which the DoC server restricts access by network address (or not at all), and the client trusts its router to advertise a suitable Encrypted DNS server.

1. Client: Joins a network.

2. Local router: Sends out an IPv6 Router Advertisement (RA) with Encrypted DNS option (see Section 6 of [RFC9463]).

   Next to the network address, this conveys Service Parameters indicating DoC as well as a CWT Claims Set (CCS, [RFC8392]) that is to be used as an EDHOC credential.

3. Client starts EDHOC with the server at the indicated address. The client uses an ephemeral identity (i.e., authenticates with a CCS by value) and verifies that the DoC server is in possession of the key indicated in the CCS without explicit transmission of the CCS.

4.1.2. DHCP discovered server with ACE details

In which both the DoC client and server have a preconfigured security association with an ACE server, and trust no one else.

1. Client: Requests an address using DHCP

2. DHCP server: Offers an address along with the DHCPv6 Encrypted DNS Option (see Section 5 of [RFC9463]).

   The option contains an address as well as an indication that ACE is used, along with sufficient data for the client to obtain an ACE token.

This includes hints like the ACE Request Creation hints: the address of the AS and an identifier of the DoC server understood by the AS (the "aud"ience). The address of the AS should be provided in some resolved form, given that DNS is being bootstrapped.

3. Client requests token from AS:

   "I need a token for a host that is authorized to be my DNS server with me being authorized to use it; these hints were presented for me to obtain it."

4. AS verifies that the hint represents a recognized DNS server, that the client is authorized to use it, and issues a token for a suitable ACE profile (e.g. ACE OSCORE profile or ACE EDHOC profile).

5. Client establishes a security context with the DoC server as per the profile.

5. Security Considerations

TODO Security

6. IANA Considerations

This document has no IANA considerations.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC9460] Schwartz, B., Bishop, M., and E. Nygren, "Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records)", RFC 9460, DOI 10.17487/RFC9460, November 2023, <https://www.rfc-editor.org/rfc/rfc9460>.

[RFC9461] Schwartz, B., "Service Binding Mapping for DNS Servers", RFC 9461, DOI 10.17487/RFC9461, November 2023, <https://www.rfc-editor.org/rfc/rfc9461>.

[RFC9462] Pauly, T., Kinnear, E., Wood, C. A., McManus, P., and T. Jensen, "Discovery of Designated Resolvers", RFC 9462, DOI 10.17487/RFC9462, November 2023, <https://www.rfc-editor.org/rfc/rfc9462>.

[RFC9463] Boucadair, M., Ed., Reddy.K, T., Ed., Wing, D., Cook, N., and T. Jensen, "DHCP and Router Advertisement Options for the Discovery of Network-designated Resolvers (DNR)", RFC 9463, DOI 10.17487/RFC9463, November 2023, <https://www.rfc-editor.org/rfc/rfc9463>.

7.2. Informative References

[I-D.amsuess-core-coap-over-gatt] Amsテシss, C., "CoAP over GATT (Bluetooth Low Energy Generic Attributes)", Work in Progress, Internet-Draft, draft-amsuess-core-coap-over-gatt-07, 25 September 2024, <https://datatracker.ietf.org/doc/html/draft-amsuess-core-coap-over-gatt-07>.

[I-D.ietf-ace-edhoc-oscore-profile] Selander, G., Mattsson, J. P., Tiloca, M., and R. Hテカglund, "Ephemeral Diffie-Hellman Over COSE (EDHOC) and Object Security for Constrained Environments (OSCORE) Profile for Authentication and Authorization for Constrained Environments (ACE)", Work in Progress, Internet-Draft, draft-ietf-ace-edhoc-oscore-profile-08, 7 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-ace-edhoc-oscore-profile-08>.

[I-D.ietf-core-coap-dtls-alpn] Lenders, M. S., Amsテシss, C., Schmidt, T. C., and M. Wテ、hlisch, "ALPN ID Specification for CoAP over DTLS", Work in Progress, Internet-Draft, draft-ietf-core-coap-dtls-alpn-04, 1 April 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-core-coap-dtls-alpn-04>.

[I-D.ietf-core-dns-over-coap] Lenders, M. S., Amsテシss, C., Gテシndoト斂n, C., Schmidt, T. C., and M. Wテ、hlisch, "DNS over CoAP (DoC)", Work in Progress, Internet-Draft, draft-ietf-core-dns-over-coap-15, 19 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-core-dns-over-coap-15>.

[I-D.ietf-core-transport-indication]
Amsテシss, C. and M. S. Lenders, "CoAP Transport Indication", Work in Progress, Internet-Draft, draft-ietf-core-transport-indication-08, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-core-transport-indication-08>.

[lwm2m] OMA SpecWorks, "White Paper 寰Lightweight M2M 1.1", October 2018, <https://omaspecworks.org/white-paper-lightweight-m2m-1-1/>.

[RFC7228] Bormann, C., Ersue, M., and A. Keranen, "Terminology for Constrained-Node Networks", RFC 7228, DOI 10.17487/RFC7228, May 2014, <https://www.rfc-editor.org/rfc/rfc7228>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/rfc/rfc7252>.

[RFC7301] Friedl, S., Popov, A., Langley, A., and E. Stephan, "Transport Layer Security (TLS) Application-Layer Protocol Negotiation Extension", RFC 7301, DOI 10.17487/RFC7301, July 2014, <https://www.rfc-editor.org/rfc/rfc7301>.

[RFC7858] Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., and P. Hoffman, "Specification for DNS over Transport Layer Security (TLS)", RFC 7858, DOI 10.17487/RFC7858, May 2016, <https://www.rfc-editor.org/rfc/rfc7858>.

[RFC7959] Bormann, C. and Z. Shelby, Ed., "Block-Wise Transfers in the Constrained Application Protocol (CoAP)", RFC 7959, DOI 10.17487/RFC7959, August 2016, <https://www.rfc-editor.org/rfc/rfc7959>.

[RFC8323] Bormann, C., Lemay, S., Tschofenig, H., Hartke, K., Silverajan, B., and B. Raymor, Ed., "CoAP (Constrained Application Protocol) over TCP, TLS, and WebSockets", RFC 8323, DOI 10.17487/RFC8323, February 2018, <https://www.rfc-editor.org/rfc/rfc8323>.

[RFC8392] Jones, M., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "CBOR Web Token (CWT)", RFC 8392, DOI 10.17487/RFC8392, May 2018, <https://www.rfc-editor.org/rfc/rfc8392>.

[RFC8484] Hoffman, P. and P. McManus, "DNS Queries over HTTPS (DoH)", RFC 8484, DOI 10.17487/RFC8484, October 2018, <https://www.rfc-editor.org/rfc/rfc8484>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/rfc/rfc8613>.

[RFC9203] Palombini, F., Seitz, L., Selander, G., and M. Gunnarsson, "The Object Security for Constrained RESTful Environments (OSCORE) Profile of the Authentication and Authorization for Constrained Environments (ACE) Framework", RFC 9203, DOI 10.17487/RFC9203, August 2022, <https://www.rfc-editor.org/rfc/rfc9203>.

[RFC9250] Huitema, C., Dickinson, S., and A. Mankin, "DNS over Dedicated QUIC Connections", RFC 9250, DOI 10.17487/RFC9250, May 2022, <https://www.rfc-editor.org/rfc/rfc9250>.

[RFC9528] Selander, G., Preu Mattsson, J., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", RFC 9528, DOI 10.17487/RFC9528, March 2024, <https://www.rfc-editor.org/rfc/rfc9528>.

Appendix A. Change Log

A.1. Since draft-lenders-core-dnr-05 (https://datatracker.ietf.org/doc/html/draft-lenders-core-dnr-05)

* Nits
* Moving GitHub repo to netd-tud org

A.2. Since draft-lenders-core-dnr-04 (https://datatracker.ietf.org/doc/html/draft-lenders-core-dnr-04)

* Avoid the term "security mode" as it has a specific definition in RFC 7252

A.3. Since draft-lenders-core-dnr-03 (https://datatracker.ietf.org/doc/html/draft-lenders-core-dnr-03)

* Update [I-D.ietf-core-coap-dtls-alpn] reference
* intro: overhaul explanation of OSCORE setup

* objectives: Be open on ACE profiles

* Add scenarios

A.4. Since draft-lenders-core-dnr-02 (https://datatracker.ietf.org/doc/html/draft-lenders-core-dnr-02)

* Forward reference to upcoming changes in [I-D.ietf-core-transport-indication] updated

A.5. Since draft-lenders-core-dnr-01 (https://datatracker.ietf.org/doc/html/draft-lenders-core-dnr-01)

* Remove parts specified in [I-D.ietf-core-transport-indication]

* Remove parts specified in [I-D.ietf-core-coap-dtls-alpn]

* Remove solution sketches, set objectives to solve problem space

A.6. Since draft-lenders-core-dnr-00 (https://datatracker.ietf.org/doc/html/draft-lenders-core-dnr-00)

* IANA has processed the "co" ALPN and it is now added to the registry

Acknowledgments

TODO acknowledge.

Authors' Addresses

Martine Sophie Lenders
TUD Dresden University of Technology
Helmholtzstr. 10
D-01069 Dresden
Germany
Email: martine.lenders@tu-dresden.de

Christian Amsss
Email: christian@amsuess.com

Thomas C. Schmidt
HAW Hamburg
Email: t.schmidt@haw-hamburg.de

Matthias Whlisch
TUD Dresden University of Technology & Barkhausen Institut
Helmholtzstr. 10
D-01069 Dresden
Germany
Email: m.waehlisch@tu-dresden.de