Constrained RESTful Environments
Internet-Draft
Intended status: Informational
Expires: 3 October 2025

M. S. Lenders
TU Dresden
C. Amsüss

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

1 April 2025

ALPN ID Specification for CoAP over DTLS
draft-ietf-core-coap-dtls-alpn-04

Abstract

This document specifies an Application-Layer Protocol Negotiation (ALPN) ID for transport-layer-secured Constrained Application Protocol (CoAP) services.

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://core-wg.github.io/coap-dtls-alpn/draft-ietf-core-coap-dtls-alpn.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-core-coap-dtls-alpn/.

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/core-wg/coap-dtls-alpn.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Application-Layer Protocol Negotiation (ALPN) enables communicating parties to agree on an application-layer protocol during a Transport Layer Security (TLS) handshake using an ALPN ID [RFC7301]. This ALPN ID can be discovered for services as part of Service Bindings (SVCB) via the DNS, using SVCB resource records with the "alpn" Service Parameter Keys [RFC9460]. As an example, applications that use the Constrained Application Protocol (CoAP) [RFC7252] can obtain this

information as part of the discovery of DNS over CoAP (DoC) servers (see Section 3.2 of [I-D.ietf-core-dns-over-coap]) that deploy TLS [RFC8446] or Datagram Transport Layer Security (DTLS) [RFC6347] [RFC9147] to secure their messages. This document specifies an ALPN ID for CoAP services that are secured by transport layer security using DTLS. An ALPN ID for CoAP services secured by TLS has already been specified in [RFC8323].

2. Application-Layer Protocol Negotiation (ALPN) IDs

For CoAP over TLS, an ALPN ID was defined as "coap" in [RFC8323]. As it is not advisable to re-use the same ALPN ID for a different transport layer, an ALPN for CoAP over DTLS is registered in Section 4.1.

ALPN ID values have variable length. For CoAP over DTLS, a short value ("co") is allocated, as this can avoid fragmentation of Client Hello and Server Hello messages in constrained networks with link-layer fragmentation, such as 6LoWPAN [RFC4944].

To discover CoAP services that secure their messages with TLS or DTLS, the ALPN IDs "coap" and "co" can be used, respectively, in the same manner as for any other service secured with transport layer security, as described in [RFC9460]. The discovery of CoAP services that rely on other security mechanisms is out of the scope of this document.

3. Security Considerations

Any security considerations on ALPN (see [RFC7301]) and SVCB resource records (see [RFC9460]) also apply to this document.

4. IANA Considerations

// RFC Ed.: throughout this section, please replace RFC-XXXX with the
// RFC number of this specification and remove this note.

This document has the following actions for IANA.

4.1. TLS ALPN for CoAP

The following entry has been added to the "TLS Application-Layer Protocol Negotiation (ALPN) Protocol IDs" registry, which is part of the "Transport Layer Security (TLS) Extensions" registry group.

* Protocol: CoAP (over DTLS)

* Identification sequence: 0x63 0x6f ("co")

* Reference: [RFC7252] and [RFC-XXXX]

Note that [RFC7252] does not define the use of the ALPN TLS extension during the DTLS connection handshake. This document does not change this behavior, and thus does not establish any rules like those in Section 8.2 of [RFC8323].

5. References

5.1. Normative References

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, DOI 10.17487/RFC6347, January 2012, <https://www.rfc-editor.org/rfc/rfc6347>.

[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>.

[RFC9147] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", RFC 9147, DOI 10.17487/RFC9147, April 2022, <https://www.rfc-editor.org/rfc/rfc9147>.

[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>.

5.2. Informative References

[I-D.ietf-core-dns-over-coap] Lenders, M. S., Ams端ss, C., G端ndoト歛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-13, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-core-dns-over-coap-13>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <https://www.rfc-editor.org/rfc/rfc4944>.

[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>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

Appendix A. Change Log

A.1. Since draft-ietf-core-coap-dtls-alpn-03 (https://datatracker.ietf.org/doc/draft-ietf-core-coap-dtls-alpn/03/)

* Make DTLS references normative

A.2. Since draft-ietf-core-coap-dtls-alpn-02 (https://datatracker.ietf.org/doc/draft-ietf-core-coap-dtls-alpn/02/)

* Address shepherd review

A.3. Since draft-ietf-core-coap-dtls-alpn-01 (https://datatracker.ietf.org/doc/draft-ietf-core-coap-dtls-alpn/01/)

* Address review by Esko Dijk

* Address review by Marco Tiloca

A.4. Since draft-ietf-core-coap-dtls-alpn-00 (https://datatracker.ietf.org/doc/draft-ietf-core-coap-dtls-alpn/00/)

* Fix ALPN ID for CoAP over TLS

* Change intended status to Informational

Acknowledgments

We like to thank Rich Salz for the expert review on the "co" ALPN ID allocation. We also like to thank Mohamed Boucadair and Ben Schwartz for their early review before WG adoption of this draft and Esko Dijk, Thomas Fossati, and Marco Tiloca for their feedback and comments.

Authors' Addresses

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

Christian Amsテシss
Email: christian@amsuess.com

Thomas C. Schmidt
HAW Hamburg
Berliner Tor 7
D-20099 Hamburg
Germany
Email: t.schmidt@haw-hamburg.de

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