Internet Engineering Task Force (IETF)
Request for Comments: 9952
Category: Informational
ISSN: 2070-1721

M. S. Lenders
TU Dresden
C. Amsss

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

March 2026

Application-Layer Protocol Negotiation (ALPN) ID for CoAP over DTLS

Abstract

This document specifies an Application-Layer Protocol Negotiation (ALPN) ID for Constrained Application Protocol (CoAP) services that are secured by DTLS.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are candidates for any level of Internet Standard; see Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9952.

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 (SVCBs) 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 [RFC9953]) that deploy TLS 1.3 [RFC8446] as well as Datagram Transport Layer Security (DTLS) 1.2 or 1.3 [RFC6347] [RFC9147] to secure their messages. This document specifies an ALPN ID for CoAP services that are secured by 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 is defined as "coap" in [RFC8323]. As it is not advisable to reuse the same ALPN ID for a different transport layer, an ALPN for CoAP over DTLS is registered in Section 4.

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 TLS, 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 for ALPN (see [RFC7301]) and SVCB resource records (see [RFC9460]) also apply to this document.

4. IANA Considerations

IANA has added the following entry to the "TLS Application-Layer Protocol Negotiation (ALPN) Protocol IDs" registry in the "Transport Layer Security (TLS) Extensions" registry group.

Protocol	Identification Sequence	Reference
CoAP (over DTLS)	0x63 0x6f ("co")	[RFC7252], RFC 9952

Table 1: TLS Application-Layer Protocol Negotiation (ALPN) Protocol IDs Registry

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/info/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/info/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/info/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/info/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/info/rfc9460>.

5.2. Informative References

[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/info/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/info/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/info/rfc8446>.

[RFC9953] Lenders, M. S., Amsss, C., Gndoan, C., Schmidt, T. C., and M. Whlisch, "DNS over CoAP (DoC)", RFC 9953, DOI 10.17487/RFC9953, March 2026, <https://www.rfc-editor.org/info/rfc9953>.

Acknowledgments

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

This work was supported in parts by the German Federal Ministry of Research, Technology, and Space (BMFTR) under the grant numbers 16KIS1386K (TU Dresden) and 16KIS1387 (HAW Hamburg) within the research project PIVOT and under the grant numbers 16KIS1694K (TU Dresden) and 16KIS1695 (HAW Hamburg) within the research project C-ray4edge.

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
Berliner Tor 7
D-20099 Hamburg
Germany
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