Workgroup: ACE Working Group
Internet-Draft:
draft-ietf-ace-extend-dtls-authorize-02
Updates: draft-ietf-ace-dtls-authorize
(if approved)
Published: 7 March 2022
Intended Status: Standards Track
Expires: 8 September 2022
Authors: O. Bergmann TZI
J. Preuß Mattsson Ericsson
G. Selander Ericsson

Extension of the CoAP-DTLS Profile for ACE to TLS

Abstract

This document updates the CoAP-DTLS profile for ACE [I-D.ietf-ace-dtls-authorize] by specifying that the profile applies to TLS as well as DTLS.

Discussion Venues

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

Discussion of this document takes place on the Authentication and Authorization for Constrained Environments Working Group mailing list (ace@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/ace/.

Source for this draft and an issue tracker can be found at https://github.com/ace-wg/ace-extend-dtls-authorize.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 8 September 2022.

Table of Contents

1. Introduction

[I-D.ietf-ace-dtls-authorize] only specifies the use of DTLS [RFC6347] but works equally well for TLS [RFC8446]. For many constrained implementations, CoAP over UDP [RFC7252] is the first choice, but when deploying ACE in networks controlled by other entities (such as the Internet), UDP might be blocked on the path between the client and the RS, and the client might have to fall back to CoAP over TCP [RFC8323] for NAT or firewall traversal. This feature is supported by the OSCORE profile [I-D.ietf-ace-oscore-profile] but is lacking in the DTLS profile.

This document updates [I-D.ietf-ace-dtls-authorize] by specifying that the profile applies to TLS as well as DTLS. The same access rights are valid in case transport layer security is provided by either DTLS or TLS, and the same access token can be used. Therefore, the value coap_dtls in the ace_profile parameter of an AS-to-Client response or in the ace_profile claim of an access token indicates that either DTLS or TLS can be used for transport layer security.

2. Terminology

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.

Readers are expected to be familiar with the terms and concepts described in [I-D.ietf-ace-oauth-authz] and [I-D.ietf-ace-dtls-authorize].

3. Connection Establishment

Following the procedures defined in [I-D.ietf-ace-dtls-authorize], a Client can retrieve an Access Token from an Authorization Server (AS) in order to establish a security association with a specific Resource Server. The ace_profile parameter in the Client-to-AS request and AS-to-client response is used to determine the ACE profile that the Client uses towards the Resource Server (RS).

In case the ace_profile parameter indicates the use of the DTLS profile for ACE as defined in [I-D.ietf-ace-dtls-authorize], the Client **MAY** try to connect to the Resource Server via TLS, or try TLS and DTLS in parallel to accelerate the session setup.

As resource-constrained devices are not expected to support both transport layer security mechanisms, a Client that implements either TLS or DTLS but not both might fail in establishing a secure communication channel with the Resource Server altogether. This error **SHOULD** be handled by the Client in the same way as unsupported ACE profiles. If the Client is modified accordingly or it learns that the Resource Server has been, the Client may try to connect to the Resource Server using the transport layer security mechanism that was previously not mutually supported.

Note that a communication setup with an a priori unknown Resource Server typically employs an initial unauthorized resource request as illustrated in Section 2 of [I-D.ietf-ace-dtls-authorize]. If this message exchange succeeds, the Client **SHOULD** first use the same underlying transport protocol for the establishment of the security association as well (i.e., DTLS for UDP, and TLS for TCP).

As a consequence, the selection of the transport protocol used for the initial unauthorized resource request also depends on the transport layer security mechanism supported by the Client. Clients that support either DTLS or TLS but not both **SHOULD** use the transport protocol underlying the supported transport layer security mechanism also for an initial unauthorized resource request.

4. IANA Considerations

The following updates have been done for the "ACE Profiles" registry for the profile with Profile ID 1 and Profile name coap_dtls:

Note to RFC Editor: Please replace all occurrences of "[RFC-XXXX]" with the RFC number of this specification and delete this paragraph.

Description: Profile for delegating client Authentication and Authorization for Constrained Environments by establishing a Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) channel between resource-constrained nodes.

Change Controller: IESG

Reference: [RFC-XXXX]

5. Security Considerations

The security consideration and requirements in TLS 1.3 [RFC8446] and BCP 195 [RFC7525] [RFC8996] also apply to this document.

6. References

6.1. Normative References

[I-D.ietf-ace-dtls-authorize] Gerdes, S., Bergmann, O., Bormann, C., Selander, G., and L. Seitz, "Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE)", Work in Progress, Internet-Draft, draft-ietf-ace-dtls-authorize-18, 4 June 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-dtls-authorize-18.txt>.

[I-D.ietf-ace-oauth-authz] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)", Work in Progress, Internet-Draft, draft-ietf-ace-oauth-authz-46, 8 November 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-oauth-authz-46.txt>.

[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/info/rfc2119>.

[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>.

[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/info/rfc8174>.

[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>.

6.2. Informative References

[I-D.ietf-ace-oscore-profile] Palombini, F., Seitz, L., Selander, G., and M. Gunnarsson, "OSCORE Profile of the Authentication and Authorization for Constrained Environments Framework", Work in Progress, Internet-Draft, draft-ietf-ace-oscore-profile-19, 6 May 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-oscore-profile-19.txt>.

[RFC7525] Sheffer, Y., Holz, R., and P. Saint-Andre, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 7525, DOI 10.17487/RFC7525, May 2015, <https://www.rfc-editor.org/info/rfc7525>.

[RFC8996] Moriarty, K. and S. Farrell, "Deprecating TLS 1.0 and TLS 1.1", BCP 195, RFC 8996, DOI 10.17487/RFC8996, March 2021, <https://www.rfc-editor.org/info/rfc8996>.

Acknowledgments

The authors would like to thank Marco Tiloca for reviewing this specification.

Authors' Addresses

Olaf Bergmann
Universität Bremen TZI
Bremen, D-28359

Germany

Email: bergmann@tzi.org

John Preuß Mattsson
Ericsson AB
SE-164 80 Stockholm
Sweden

Email: john.mattsson@ericsson.com

Göran Selander
Ericsson AB
SE-164 80 Stockholm
Sweden

Email: goran.selander@ericsson.com