Workgroup: ACE Working Group
Internet-Draft:
draft-ietf-ace-extend-dtls-authorize-07
Updates: 9202 (if approved)
Published: 9 March 2023
Intended Status: Standards Track
Expires: 10 September 2023
Authors: O. Bergmann (TZI), J. Preuß Mattsson (Ericsson), G. Selander (Ericsson)

Extension of the Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE) to Transport Layer Security (TLS)

Abstract

This document updates the Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE) specified in RFC 9202 by specifying that the profile applies to Transport Layer Security (TLS) as well as Datagram TLS (DTLS).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The Authentication and Authorization for Constrained Environments (ACE) framework [RFC9200] defines an architecture for lightweight authentication between Client, Resource Server (RS), and Authorization Server (AS) where the Client and RS may be constrained. The Datagram Transport Layer Security (DTLS) Profile for Authentication and Authorization for Constrained Environments (ACE) [RFC9202] only specifies the use of Datagram Transport Layer Security (DTLS) [RFC9147] for transport-layer security between the nodes in the ACE architecture but works equally well for Transport Layer Security (TLS) [RFC8446]. For many constrained implementations, Constrained Application Protocol (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 Resource Server, and the Client might have to fall back to CoAP over TCP [RFC8323] for NAT or firewall traversal. This dual support for security over TCP as well as UDP is already supported by the Object Security for Constrained RESTful Environments (OSCORE) profile [RFC9203].

This document updates [RFC9202] by specifying that the profile applies to TLS as well as DTLS. It only impacts the transport layer security channel between Client and Resource Server. The same access rights are valid in case transport layer security is provided by either DTLS or TLS. The same access token can be used by either DTLS or TLS between a given (Client, RS) pair. Therefore, the value coap_dtls in the ace_profile parameter of an Authorization Server to Client (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 [RFC9200] and [RFC9202].

3. Specific Changes to RFC 9202

The main changes to [RFC9202] specified in this document are limited to replacing "DTLS" with "DTLS/TLS" throughout the document. This essentially impacts the use of secure transport as described in the sections 3.2.2, 3.3.2, 4, and 5.

In addition to this, the Client and Resource Server behavior is updated to describe the case where either or both DTLS and TLS may be available, as described in the following section.

4. Connection Establishment

Following the procedures defined in [RFC9202], a Client can retrieve an Access Token from an Authorization Server 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.

The ace_profile parameter indicates the use of the DTLS profile for ACE as defined in [RFC9202]. Therefore, the Client typically first tries using DTLS to connect to the Resource Server. If this fails the Client **MAY** try to connect to the Resource Server via TLS.

As resource-constrained devices are not expected to support both transport layer security mechanisms, Clients and Resource Servers **SHOULD** support DTLS and **MAY** support TLS. A Client that implements either TLS or DTLS but not both might fail in establishing a secure communication channel with the Resource Server altogether. Non-constrained Clients and Resource Servers **SHOULD** support both TLS and DTLS.

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 [RFC9202]. If this message exchange succeeds, the Client **SHOULD** first use the same underlying transport protocol also for the establishment of the security association to the Resource Server (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 to the Resource Server as in Section 2 of [RFC9202].

5. IANA Considerations

The following updates have been done to the "ACE Profiles" registry for the profile with a "CBOR Value" field value of 1 and "Name" of "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: [RFC9202] [RFC-XXXX]

6. Security Considerations

The security consideration and requirements in [RFC9202], TLS 1.3 [RFC8446], and BCP 195 [RFC8996] [RFC9325] also apply to this document.

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/info/rfc2119>.

[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>.

[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>.

[RFC9200] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments Using the OAuth 2.0 Framework (ACE-OAuth)", RFC 9200, DOI 10.17487/RFC9200, August 2022, <https://www.rfc-editor.org/info/rfc9200>.

[RFC9202] 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)", RFC 9202, DOI 10.17487/RFC9202, August 2022, <https://www.rfc-editor.org/info/rfc9202>.

7.2. Informative References

[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>.

[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/info/rfc9203>.

[RFC9325] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", BCP 195, RFC 9325, DOI 10.17487/RFC9325, November 2022, <https://www.rfc-editor.org/info/rfc9325>.

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