Workgroup: Network Working Group
Internet-Draft:
draft-bergmann-ace-extend-dtls-authorize-00
Updates: draft-ietf-ace-dtls-authorize
        (if approved)
Published: 8 November 2021
Intended Status: Standards Track
Expires: 12 May 2022

Authors: O. Bergmann   J. Preuß Mattsson   G. Selander
         TZI   Ericsson   Ericsson

Extension of the ACE CoAP-DTLS Profile to TLS

Abstract

This document updates the ACE CoAP-DTLS profile by specifying that the profile applies to TLS as well as DTLS.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

[I-D.ietf-ace-dtls-authorize] only specifies use of DTLS [I-D.ietf-tls-dtls13] but works equally well for TLS. 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 from 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 either DTLS or TLS, and the same access token can be used.

2. IANA Considerations

No IANA Considerations.

3. Security Considerations

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

4. References

4.1. 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-tls-dtls13] Rescorla, E., Tschofenig, H., and N. Modadugu, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3", Work in Progress, Internet-Draft, draft-ietf-tls-dtls13-43, 30 April 2021, <https://www.ietf.org/internet-drafts/draft-ietf-tls-dtls13-43.txt>.

[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>.

[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>.

4.2. 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

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