Workgroup: Transport Layer Security
Internet-Draft:
draft-whited-tls-channel-bindings-for-tls13-02
Published: 4 May 2020
Intended Status: Experimental
Expires: 5 November 2020
Authors: S. Whited

Channel Bindings for SCRAM over TLS 1.3

Abstract

This document defines a channel binding type, tls-scram-exporter, that is compatible with SCRAM [RFC5802] and TLS 1.3 [RFC8446] in accordance with On Channel Binding [RFC5056].

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 5 November 2020.

Table of Contents

1. Introduction

After problems were found with the channel binding types defined in [RFC5929] they were not defined for TLS 1.3 [RFC8446]. To facilitate channel binding with TLS 1.3, a new channel binding type using keying material obtained from [RFC5705] is needed.

1.1. Conventions and Terminology

Throughout this document the acronym "EKM" is used to refer to Exported Keying Material as defined in [RFC5705].

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.

2. The 'tls-scram-exporter' Channel Binding Type

IANA will register the 'tls-scram-exporter' channel binding type to match the description below.

Description: The EKM value obtained from the current TLS connection.

The EKM is obtained using the keying material exporters for TLS as defined in [RFC5705] by supplying the following inputs. The

definition of "client-first-message-bare" and "server-first-message" can be found in [RFC5802].

Label: The ASCII string "EXPORTER-SCRAM-Channel-Binding" with no terminating NUL.

Context value: client-first-message-bare + "," + server-first-message

Length: 32 bytes.

When TLS renegotiation is enabled channel binding using the "tls-scram-exporter" type is not define and **MUST NOT** be supported.

3. Security Considerations

While it is possible to use this channel binding mechanism with TLS versions below 1.3, extra precaution must be taken to ensure that the chosen cipher suites always result in unique master secrets. For more information see the Security Considerations section of [RFC5705].

The Security Considerations sections of [RFC5056], [RFC5705], [RFC5802], and [RFC8446] apply to this document.

4. IANA Considerations

4.1. Registration of Channel Binding Type

This document adds the following registration in the "Channel-Binding Types" registry:

Subject:
Registration of channel binding tls-scram-exporter

Channel binding unique prefix: tls-scram-exporter

Channel binding type: unique

Channel type: TLS [RFC8446]

Published specification: draft-whited-tls-channel-bindings-for-tls13-00

Channel binding is secret: no

Description: <See specification>

Intended usage: COMMON

Person and email address to contact for further information: Sam Whited <sam@samwhited.com>.

Owner/Change controller name and email address: IESG.

Expert reviewer name and contact information: IETF TLS WG (tls@ietf.org, failing that, ietf@ietf.org).

Note: See the published specification for advice on the applicability of this channel binding type.

4.2. Registration of Channel Binding TLS Exporter Label

This document adds the following registration in the "TLS Exporter Labels" registry:

Value: EXPORTER-SCRAM-Channel-Binding

DTLS-OK: Y

Recommended: N

Reference: This document

5. References

5.1. 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>.

[RFC5056] Williams, N., "On the Use of Channel Bindings to Secure Channels", RFC 5056, DOI 10.17487/RFC5056, November 2007, <https://www.rfc-editor.org/info/rfc5056>.

[RFC5705] Rescorla, E., "Keying Material Exporters for Transport Layer Security (TLS)", RFC 5705, DOI 10.17487/RFC5705, March 2010, <https://www.rfc-editor.org/info/rfc5705>.

[RFC5802] Newman, C., Menon-Sen, A., Melnikov, A., and N. Williams, "Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms", RFC 5802, DOI 10.17487/RFC5802, July 2010, <https://www.rfc-editor.org/info/rfc5802>.

[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>.

[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>.

5.2. Informative References

[RFC5929] Altman, J., Williams, N., and L. Zhu, "Channel Bindings for TLS", RFC 5929, DOI 10.17487/RFC5929, July 2010, <https://www.rfc-editor.org/info/rfc5929>.

Author's Address

Sam Whited
Atlanta, GA
United States of America

Email: sam@samwhited.com
URI: https://blog.samwhited.com/