Workgroup: Transport Layer Security
Internet-Draft:
draft-ietf-kitten-tls-channel-bindings-for-
tls13-06
Updates: 5801, 5802, 5929, 8446 (if approved)
Published: 26 May 2021
Intended Status: Standards Track
Expires: 27 November 2021
Authors: S. Whited

Channel Bindings for TLS 1.3

Abstract

This document defines a channel binding type, tls-exporter, that is compatible with TLS 1.3 in accordance with RFC 5056, On Channel Binding. Furthermore it updates the "default" channel binding to the new binding for versions of TLS greater than 1.2. This document updates [RFC5801], [RFC5802], [RFC5929], and [RFC8446].

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The "unique" channel binding types defined in [RFC5929] were found
to be vulnerable to the "triple handshake vulnerability" [TRIPLE-
HANDSHAKE] without the extended master secret extension defined in
[RFC7627]. Because of this they were not defined for TLS 1.3 (see
[RFC8446] section C.5). To facilitate channel binding with TLS 1.3,
a new channel binding type 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-exporter' Channel Binding Type

Channel binding mechanisms are not useful until TLS implementations
expose the required data. To facilitate this, "tls-exporter" uses
exported keying material (EKM) which is already widely exposed by
TLS implementations. The EKM is obtained using the keying material
exporters for TLS as defined in [RFC5705] and [RFC8446] section 7.5
by supplying the following inputs:

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

Context value:
Empty context value.

Length: 32 bytes.

In previous versions of TLS the "tls-unique" channel binding type
was defined as the default channel binding if no mechanism was
defined for negotiating a different channel binding. Because "tls-
unique" is not defined for TLS 1.3, the default channel binding
mechanism for TLS versions 1.3 and greater **MUST** be "tls-exporter".

3. Security Considerations

Channel bindings do not leak secret information about the channel
and are considered public. Implementations MUST NOT use the channel
binding to protect secret information.

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

3.1. Use with Legacy TLS

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].

When TLS renegotiation is enabled the "tls-exporter" channel binding
type is not defined and implementations **MUST NOT** support it.

In general, users wishing to take advantage of channel binding
should upgrade to TLS 1.3 or later.

The derived data **MUST NOT** be used for any purpose other than channel
bindings as described in [RFC5056].

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-exporter

Channel binding unique prefix: tls-exporter

Channel binding type: unique

Channel type:

TLS [RFC8446]

Published specification: draft-ietf-kitten-tls-channel-bindings-
    for-tls13-06

Channel binding is secret: no

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

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 KITTEN or TLS WG
    (kitten@ietf.org or 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-Channel-Binding

DTLS-OK: Y

Recommended: Y

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>.

[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

[RFC5801] Josefsson, S. and N. Williams, "Using Generic Security
           Service Application Program Interface (GSS-API)
           Mechanisms in Simple Authentication and Security Layer
           (SASL): The GS2 Mechanism Family", RFC 5801, DOI
           10.17487/RFC5801, July 2010, <https://www.rfc-editor.org/
           info/rfc5801>.

[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>.

[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>.

[RFC7627] Bhargavan, K., Ed., Delignat-Lavaud, A., Pironti, A.,
           Langley, A., and M. Ray, "Transport Layer Security (TLS)
           Session Hash and Extended Master Secret Extension", RFC
           7627, DOI 10.17487/RFC7627, September 2015, <https://
           www.rfc-editor.org/info/rfc7627>.

[TRIPLE-HANDSHAKE] Bhargavan, K., Delignat-Lavaud, A., Fournet, C.,
           Pironti, A., and P. Strub, "Password Storage", March
           2014, <https://www.mitls.org/pages/attacks/3SHAKE>.

Author's Address

    Sam Whited
    Atlanta, GA
    United States of America

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