Transport Layer Security
Internet-Draft
Updates: 5802,5929,8446 (if approved)
Intended status: Standards Track
Expires: November 26, 2021

S. Whited

May 25, 2021

Channel Bindings for TLS 1.3
draft-ietf-kitten-tls-channel-bindings-for-tls13-04

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 [RFC5802], [RFC5929], and [RFC8446].

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 November 26, 2021.

Copyright Notice

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

1.

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.

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.

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:

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

be "tls-exporter".

3.

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.

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

support it.

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

The derived data

be used for any purpose other than channel bindings as described in [RFC5056].

4.

4.1.

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

4.2.

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

5. References

Author's Address

Sam Whited
Atlanta GA
USA

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