Using TLS 1.3 with HTTP/2

draft-davidben-http2-tls13-00

Abstract

This document clarifies the use of TLS 1.3 post-handshake authentication and key update with HTTP/2.

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 October 3, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.
1. Introduction

TLS 1.2 [RFC5246] and earlier support renegotiation, a mechanism for changing parameters and keys partway through a connection. This was sometimes used to implement reactive client authentication in HTTP/1.1 [RFC7230], where the server decides whether to request a client certificate based on the HTTP request.

HTTP/2 [RFC7540] multiplexes multiple HTTP requests over a single connection, which is incompatible with this. Clients cannot correlate the certificate request with the HTTP request which triggered it. Thus, section 9.2.1 of [RFC7540] forbids renegotiation.

TLS 1.3 [RFC8446] updates TLS 1.2 to remove renegotiation in favor of separate post-handshake authentication and key update mechanisms. The former shares the same problems with multiplexed protocols, but has a different name. This makes it ambiguous whether post-handshake authentication is allowed in TLS 1.3.

This document clarifies that the prohibition applies to post-handshake authentication but not to key updates.

2. Requirements Language

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] when, and only when, they appear in all capitals, as shown here.

3. Post-Handshake Authentication in HTTP/2

The prohibition on renegotiation in section 9.2.1 of [RFC7540] additionally applies to TLS 1.3 post-handshake authentication. HTTP/2 servers MUST NOT send post-handshake TLS 1.3 CertificateRequest messages. HTTP/2 clients MUST treat TLS 1.3 post-
handshake authentication as a connection error (see section 5.4.1 of [RFC7540]) of type PROTOCOL_ERROR.

[RFC7540] permitted renegotiation before the HTTP/2 connection preface to provide confidentiality of the client certificate. TLS 1.3 encrypts the client certificate in the initial handshake, so this is no longer necessary. HTTP/2 servers MUST NOT send post-handshake TLS 1.3 CertificateRequest messages before the connection preface.

The above applies even if the client offered the "post_handshake_auth" TLS extension. This extension is advertised independently of the selected ALPN protocol [RFC7301], so it is not sufficient to resolve the conflict with HTTP/2. HTTP/2 clients that also offer other ALPN protocols, notably HTTP/1.1, in a TLS ClientHello MAY include the "post_handshake_auth" extension to support those other protocols. This does not indicate support in HTTP/2.

4. Key Updates in HTTP/2

Section 9.2.1 of [RFC7540] does not extend to TLS 1.3 KeyUpdate messages. HTTP/2 implementations MUST support key updates when TLS 1.3 is negotiated.

5. Security Considerations

This document clarifies how to use HTTP/2 with TLS 1.3 and resolves a compatibility concern when supporting post-handshake authentication with HTTP/1.1. This lowers the barrier for deploying TLS 1.3, a major security improvement over TLS 1.2. Permitting key updates allows key material to be refreshed in long-lived HTTP/2 connections.

6. IANA Considerations

This document has no IANA actions.

7. Normative References


Author’s Address

David Benjamin
Google LLC

Email: davidben@google.com