Workgroup: PCE
Internet-Draft: draft-dhody-pce-pceps-tls13-01
Published: 20 October 2022
Intended Status: Standards Track
Expires: 23 April 2023
Authors: D. Dhody S. Turner R. Housley
Huawei Technologies sn3rd Vigil Security

PCEPS with TLS 1.3

Abstract

RFC 8253 defines how to protect PCEP messages with TLS 1.2. This document describes how to protect PCEP messages with TLS 1.3.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Path Computation Element Working Group mailing list (pce@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/pce/.

Source for this draft and an issue tracker can be found at https://github.com/dhruvdhody/draft-dhody-pce-pceps-tls13.

Status of This Memo

This Internet-Draft will expire on 23 April 2023.

Copyright Notice

Table of Contents

1. Introduction

[RFC8253] defines how to protect PCEP messages [RFC5440] with TLS 1.2 [RFC5246]. This document describes defines how to protect PCEP messages with TLS 1.3 [I-D.ietf-tls-rfc8446bis].

[Editor's Note: The reference to [I-D.ietf-tls-rfc8446bis] could be changed to RFC 8446 incase the progress of the bis draft is slower than the progression of this document.]

This document addresses cipher suites and the use of early data, which is also known as 0-RTT data. All other provisions set forth in [RFC8253] are unchanged, including connection initiation, message framing, connection closure, certificate validation, peer identity, and failure handling.

2. Conventions and Definitions

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.

3. Early Data

Early data (aka 0-RTT data) is a mechanism defined in TLS 1.3 [I-D.ietf-tls-rfc8446bis] that allows a client to send data ("early data") as part of the first flight of messages to a server. Note that TLS 1.3 can be used without early data as per Appendix F.5 of [I-D.ietf-tls-rfc8446bis]. In fact, early data is permitted by TLS 1.3 only when the client and server share a Pre-Shared Key (PSK), either obtained externally or via a previous handshake. The client uses the PSK to authenticate the server and to encrypt the early data.

As noted in Section 2.3 of [I-D.ietf-tls-rfc8446bis], the security properties for early data are weaker than those for subsequent TLS-protected data. In particular, early data is not forward secret, and there is no protection against the replay of early data between connections. Appendix E.5 of [I-D.ietf-tls-rfc8446bis] requires applications not use early data without a profile that defines its use. This document specifies that PCEPS implementations that support TLS 1.3 **MUST NOT** use early data.

4. Cipher Suites

Implementations that support TLS 1.3 [I-D.ietf-tls-rfc8446bis] are **REQUIRED** to support the mandatory-to-implement cipher suites listed in Section 9.1 of [I-D.ietf-tls-rfc8446bis].

Implementations that support TLS 1.3 **MAY** implement additional TLS cipher suites that provide mutual authentication and confidentiality, which are required for PCEP.

PCEPS Implementations **SHOULD** follow the recommendations given in [I-D.ietf-uta-rfc7525bis].

So, this is what {{Section 9.1 of I-D.ietf-tls-rfc8446bis}} says:

> A TLS-compliant application MUST implement the TLS_AES_128_GCM_SHA256 [GCM] cipher suite and SHOULD implement the TLS_AES_256_GCM_SHA384 [GCM] and TLS_CHACHA20_POLY1305_SHA256 [RFC8439] cipher suites (see Appendix B.4).
>
> A TLS-compliant application MUST support digital signatures with rsa_pkcs1_sha256 (for certificates), rsa_pss_rsae_sha256 (for CertificateVerify and certificates), and ecdsa_secp256r1_sha256. A TLS-compliant application MUST support key exchange with secp256r1 (NIST P-256) and SHOULD support key exchange with X25519 [RFC7748].

Is there any reason to narrow the algorithm choices?

My guess is not. These ought to be available in all TLS libraries.

5. Security Considerations

The Security Considerations in TLS 1.3 are specified in [I-D.ietf-tls-rfc8446bis].

The recommendations regarding Diffie-Hellman exponent reuse are specified in Section 7.4 of [I-D.ietf-uta-rfc7525bis].

The key Security Considerations for PCEP are described in [RFC5440], [RFC8231], [RFC8281], and [RFC8283].

The Path Computation Element (PCE) defined in [RFC4655] is an entity that is capable of computing a network path or route based on a network graph, and applying computational constraints. A Path Computation Client (PCC) may make requests to a PCE for paths to be computed. PCEP is the communication protocol between a PCC and PCE and is defined in [RFC5440]. Stateful PCE [RFC8231] specifies a set of extensions to PCEP to enable control of TE-LSPs by a PCE that retains the state of the LSPs provisioned in the network (a stateful PCE). [RFC8281] describes the setup, maintenance, and teardown of LSPs initiated by a stateful PCE without the need for local configuration on the PCC, thus allowing for a dynamic network that is centrally controlled. [RFC8283] introduces the architecture for PCE as a central controller

TLS 1.3 mutual authentication is used to ensure that only authorized users and systems are able to send and receive PCEP messages. To this end, neither the PCC nor the PCE should establish a PCEPS with TLS 1.3 connection with an unknown, unexpected, or incorrectly identified peer; see Section 3.5 of [RFC5440]. If deployments make use of a trusted list of Certification Authority (CA) certificates [RFC5280], then the listed CAs should only issue certificates to parties that are authorized to access the PCE. Doing otherwise will allow certificates that were issued for other purposes to be inappropriately accepted by a PCE.

The recommendations regarding certificate revocation checking are specified in Section 7.5 of [I-D.ietf-uta-rfc7525bis].

6. IANA Considerations

There are no IANA considerations.

7. References

7.1. Normative References

[I-D.ietf-tls-rfc8446bis]
Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", Work in Progress, Internet-Draft,

draft-ietf-tls-rfc8446bis-04, 7 March 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-tls-rfc8446bis-04>.

[I-D.ietf-uta-rfc7525bis] Sheffer, Y., Saint-Andre, P., and T. Fossati, "Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)", Work in Progress, Internet-Draft, draft-ietf-uta-rfc7525bis-11, 16 August 2022, <https://datatracker.ietf.org/doc/html/draft-ietf-uta-rfc7525bis-11>.

[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/rfc/rfc2119>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC5440] Vasseur, JP., Ed. and JL. Le Roux, Ed., "Path Computation Element (PCE) Communication Protocol (PCEP)", RFC 5440, DOI 10.17487/RFC5440, March 2009, <https://www.rfc-editor.org/rfc/rfc5440>.

[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/rfc/rfc8174>.

[RFC8253] Lopez, D., Gonzalez de Dios, O., Wu, Q., and D. Dhody, "PCEPS: Usage of TLS to Provide a Secure Transport for the Path Computation Element Communication Protocol (PCEP)", RFC 8253, DOI 10.17487/RFC8253, October 2017, <https://www.rfc-editor.org/rfc/rfc8253>.

7.2. Informative References

[RFC4655] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <https://www.rfc-editor.org/rfc/rfc4655>.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/rfc/rfc5246>.

[RFC8231]
Crabbe, E., Minei, I., Medved, J., and R. Varga, "Path Computation Element Communication Protocol (PCEP) Extensions for Stateful PCE", RFC 8231, DOI 10.17487/RFC8231, September 2017, <https://www.rfc-editor.org/rfc/rfc8231>.

[RFC8281] Crabbe, E., Minei, I., Sivabalan, S., and R. Varga, "Path Computation Element Communication Protocol (PCEP) Extensions for PCE-Initiated LSP Setup in a Stateful PCE Model", RFC 8281, DOI 10.17487/RFC8281, December 2017, <https://www.rfc-editor.org/rfc/rfc8281>.

[RFC8283] Farrel, A., Ed., Zhao, Q., Ed., Li, Z., and C. Zhou, "An Architecture for Use of PCE and the PCE Communication Protocol (PCEP) in a Network with Central Control", RFC 8283, DOI 10.17487/RFC8283, December 2017, <https://www.rfc-editor.org/rfc/rfc8283>.

Acknowledgments

We would like to thank Adrian Farrel for their review.

Authors' Addresses

Dhruv Dhody
Huawei Technologies

Email: dhruv.ietf@gmail.com

Sean Turner
sn3rd

Email: sean@sn3rd.com

Russ Housley
Vigil Security, LLC
516 Dranesville Road
Herndon, VA, 20170
United States of America

Email: housley@vigilsec.com