

< draft-ietf-pce-pceps-14.txt		draft-ietf-pce-pceps-15.txt >																																																																																																																	
PCE Working Group	D. Lopez	PCE Working Group	D. Lopez																																																																																																																
Internet-Draft	O. Gonzalez de Dios	Internet-Draft	O. Gonzalez de Dios																																																																																																																
Updates: 5440 (if approved)	Telefonica I+D	Updates: 5440 (if approved)	Telefonica I+D																																																																																																																
Intended status: Standards Track	Q. Wu	Intended status: Standards Track	Q. Wu																																																																																																																
Expires: November 23, 2017	D. Dhody	Expires: February 1, 2018	D. Dhody																																																																																																																
	Huawei		Huawei																																																																																																																
	May 22, 2017		July 31, 2017																																																																																																																
Secure Transport for PCEP		Secure Transport for PCEP																																																																																																																	
draft-ietf-pce-pceps-14		draft-ietf-pce-pceps-15																																																																																																																	
Abstract		Abstract																																																																																																																	
<p>The Path Computation Element Communication Protocol (PCEP) defines the mechanisms for the communication between a Path Computation Client (PCC) and a Path Computation Element (PCE), or among PCEs. This document describe the usage of Transport Layer Security (TLS) to enhance PCEP security, hence the PCEPS acronym proposed for it. The additional security mechanisms are provided by the transport protocol supporting PCEP, and therefore they do not affect the flexibility and</p>		<p>The Path Computation Element Communication Protocol (PCEP) defines the mechanisms for the communication between a Path Computation Client (PCC) and a Path Computation Element (PCE), or among PCEs. This document describe the usage of Transport Layer Security (TLS) to enhance PCEP security, hence the PCEPS acronym proposed for it. The additional security mechanisms are provided by the transport protocol supporting PCEP, and therefore they do not affect the flexibility and</p>																																																																																																																	
skipping to change at page 1, line 43		skipping to change at page 1, line 43																																																																																																																	
<p>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 http://datatracker.ietf.org/drafts/current/.</p> <p>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."</p>		<p>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 http://datatracker.ietf.org/drafts/current/.</p> <p>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."</p>																																																																																																																	
This Internet-Draft will expire on November 23, 2017.		This Internet-Draft will expire on February 1, 2018.																																																																																																																	
Copyright Notice		Copyright Notice																																																																																																																	
<p>Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.</p> <p>This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents</p>		<p>Copyright (c) 2017 IETF Trust and the persons identified as the document authors. All rights reserved.</p> <p>This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents</p>																																																																																																																	
skipping to change at page 2, line 34		skipping to change at page 2, line 34																																																																																																																	
it for publication as an RFC or to translate it into languages other than English.		it for publication as an RFC or to translate it into languages other than English.																																																																																																																	
Table of Contents		Table of Contents																																																																																																																	
<table><tr><td>1. Introduction</td><td>3</td></tr><tr><td>2. Requirements Language</td><td>4</td></tr><tr><td>3. Applying PCEPS</td><td>4</td></tr><tr><td> 3.1. Overview</td><td>4</td></tr><tr><td> 3.2. Initiating the TLS Procedures</td><td>4</td></tr><tr><td> 3.3. The StartTLS Message</td><td>6</td></tr><tr><td> 3.4. TLS Connection Establishment</td><td>8</td></tr><tr><td> 3.5. Peer Identity</td><td>10</td></tr><tr><td> 3.6. Connection Establishment Failure</td><td>11</td></tr><tr><td>4. Discovery Mechanisms</td><td>11</td></tr><tr><td> 4.1. DANE Applicability</td><td>12</td></tr><tr><td>5. Backward Compatibility</td><td>12</td></tr><tr><td>6. IANA Considerations</td><td>12</td></tr><tr><td> 6.1. New PCEP Message</td><td>12</td></tr><tr><td> 6.2. New Error-Values</td><td>13</td></tr><tr><td>7. Security Considerations</td><td>13</td></tr><tr><td>8. Manageability Considerations</td><td>14</td></tr><tr><td> 8.1. Control of Function and Policy</td><td>14</td></tr><tr><td> 8.2. Information and Data Models</td><td>15</td></tr><tr><td> 8.3. Liveness Detection and Monitoring</td><td>15</td></tr><tr><td> 8.4. Verify Correct Operations</td><td>15</td></tr><tr><td> 8.5. Requirements on Other Protocols</td><td>15</td></tr><tr><td> 8.6. Impact on Network Operation</td><td>16</td></tr><tr><td>9. Acknowledgements</td><td>16</td></tr><tr><td>10. References</td><td>16</td></tr><tr><td> 10.1. Normative References</td><td>16</td></tr><tr><td> 10.2. Informative References</td><td>17</td></tr><tr><td>Authors' Addresses</td><td>18</td></tr></table>		1. Introduction	3	2. Requirements Language	4	3. Applying PCEPS	4	3.1. Overview	4	3.2. Initiating the TLS Procedures	4	3.3. The StartTLS Message	6	3.4. TLS Connection Establishment	8	3.5. Peer Identity	10	3.6. Connection Establishment Failure	11	4. Discovery Mechanisms	11	4.1. DANE Applicability	12	5. Backward Compatibility	12	6. IANA Considerations	12	6.1. New PCEP Message	12	6.2. New Error-Values	13	7. Security Considerations	13	8. Manageability Considerations	14	8.1. Control of Function and Policy	14	8.2. Information and Data Models	15	8.3. Liveness Detection and Monitoring	15	8.4. Verify Correct Operations	15	8.5. Requirements on Other Protocols	15	8.6. Impact on Network Operation	16	9. Acknowledgements	16	10. References	16	10.1. Normative References	16	10.2. Informative References	17	Authors' Addresses	18	<table><tr><td>1. Introduction</td><td>3</td></tr><tr><td>2. Requirements Language</td><td>4</td></tr><tr><td>3. Applying PCEPS</td><td>4</td></tr><tr><td> 3.1. Overview</td><td>4</td></tr><tr><td> 3.2. Initiating the TLS Procedures</td><td>4</td></tr><tr><td> 3.3. The StartTLS Message</td><td>7</td></tr><tr><td> 3.4. TLS Connection Establishment</td><td>11</td></tr><tr><td> 3.5. Peer Identity</td><td>13</td></tr><tr><td> 3.6. Connection Establishment Failure</td><td>14</td></tr><tr><td>4. Discovery Mechanisms</td><td>15</td></tr><tr><td> 4.1. DANE Applicability</td><td>15</td></tr><tr><td>5. Backward Compatibility</td><td>15</td></tr><tr><td>6. IANA Considerations</td><td>16</td></tr><tr><td> 6.1. New PCEP Message</td><td>16</td></tr><tr><td> 6.2. New Error-Values</td><td>16</td></tr><tr><td>7. Security Considerations</td><td>17</td></tr><tr><td>8. Manageability Considerations</td><td>18</td></tr><tr><td> 8.1. Control of Function and Policy</td><td>18</td></tr><tr><td> 8.2. Information and Data Models</td><td>19</td></tr><tr><td> 8.3. Liveness Detection and Monitoring</td><td>19</td></tr><tr><td> 8.4. Verifying Correct Operations</td><td>19</td></tr><tr><td> 8.5. Requirements on Other Protocols</td><td>19</td></tr><tr><td> 8.6. Impact on Network Operation</td><td>19</td></tr><tr><td>9. Acknowledgements</td><td>19</td></tr><tr><td>10. References</td><td>20</td></tr><tr><td> 10.1. Normative References</td><td>20</td></tr><tr><td> 10.2. Informative References</td><td>21</td></tr><tr><td>Authors' Addresses</td><td>23</td></tr></table>		1. Introduction	3	2. Requirements Language	4	3. Applying PCEPS	4	3.1. Overview	4	3.2. Initiating the TLS Procedures	4	3.3. The StartTLS Message	7	3.4. TLS Connection Establishment	11	3.5. Peer Identity	13	3.6. Connection Establishment Failure	14	4. Discovery Mechanisms	15	4.1. DANE Applicability	15	5. Backward Compatibility	15	6. IANA Considerations	16	6.1. New PCEP Message	16	6.2. New Error-Values	16	7. Security Considerations	17	8. Manageability Considerations	18	8.1. Control of Function and Policy	18	8.2. Information and Data Models	19	8.3. Liveness Detection and Monitoring	19	8.4. Verifying Correct Operations	19	8.5. Requirements on Other Protocols	19	8.6. Impact on Network Operation	19	9. Acknowledgements	19	10. References	20	10.1. Normative References	20	10.2. Informative References	21	Authors' Addresses	23
1. Introduction	3																																																																																																																		
2. Requirements Language	4																																																																																																																		
3. Applying PCEPS	4																																																																																																																		
3.1. Overview	4																																																																																																																		
3.2. Initiating the TLS Procedures	4																																																																																																																		
3.3. The StartTLS Message	6																																																																																																																		
3.4. TLS Connection Establishment	8																																																																																																																		
3.5. Peer Identity	10																																																																																																																		
3.6. Connection Establishment Failure	11																																																																																																																		
4. Discovery Mechanisms	11																																																																																																																		
4.1. DANE Applicability	12																																																																																																																		
5. Backward Compatibility	12																																																																																																																		
6. IANA Considerations	12																																																																																																																		
6.1. New PCEP Message	12																																																																																																																		
6.2. New Error-Values	13																																																																																																																		
7. Security Considerations	13																																																																																																																		
8. Manageability Considerations	14																																																																																																																		
8.1. Control of Function and Policy	14																																																																																																																		
8.2. Information and Data Models	15																																																																																																																		
8.3. Liveness Detection and Monitoring	15																																																																																																																		
8.4. Verify Correct Operations	15																																																																																																																		
8.5. Requirements on Other Protocols	15																																																																																																																		
8.6. Impact on Network Operation	16																																																																																																																		
9. Acknowledgements	16																																																																																																																		
10. References	16																																																																																																																		
10.1. Normative References	16																																																																																																																		
10.2. Informative References	17																																																																																																																		
Authors' Addresses	18																																																																																																																		
1. Introduction	3																																																																																																																		
2. Requirements Language	4																																																																																																																		
3. Applying PCEPS	4																																																																																																																		
3.1. Overview	4																																																																																																																		
3.2. Initiating the TLS Procedures	4																																																																																																																		
3.3. The StartTLS Message	7																																																																																																																		
3.4. TLS Connection Establishment	11																																																																																																																		
3.5. Peer Identity	13																																																																																																																		
3.6. Connection Establishment Failure	14																																																																																																																		
4. Discovery Mechanisms	15																																																																																																																		
4.1. DANE Applicability	15																																																																																																																		
5. Backward Compatibility	15																																																																																																																		
6. IANA Considerations	16																																																																																																																		
6.1. New PCEP Message	16																																																																																																																		
6.2. New Error-Values	16																																																																																																																		
7. Security Considerations	17																																																																																																																		
8. Manageability Considerations	18																																																																																																																		
8.1. Control of Function and Policy	18																																																																																																																		
8.2. Information and Data Models	19																																																																																																																		
8.3. Liveness Detection and Monitoring	19																																																																																																																		
8.4. Verifying Correct Operations	19																																																																																																																		
8.5. Requirements on Other Protocols	19																																																																																																																		
8.6. Impact on Network Operation	19																																																																																																																		
9. Acknowledgements	19																																																																																																																		
10. References	20																																																																																																																		
10.1. Normative References	20																																																																																																																		
10.2. Informative References	21																																																																																																																		
Authors' Addresses	23																																																																																																																		
1. Introduction		1. Introduction																																																																																																																	
<p>The Path Computation Element Communication Protocol (PCEP) [RFC5440] defines the mechanisms for the communication between a Path Computation Client (PCC) and a Path Computation Element (PCE), or between two PCEs. These interactions include requests and replies that can be critical for a sustainable network operation and adequate resource allocation, and therefore appropriate security becomes a key element in the PCE infrastructure. As the applications of the PCE</p>		<p>The Path Computation Element Communication Protocol (PCEP) [RFC5440] defines the mechanisms for the communication between a Path Computation Client (PCC) and a Path Computation Element (PCE), or between two PCEs. These interactions include requests and replies that can be critical for a sustainable network operation and adequate resource allocation, and therefore appropriate security becomes a key element in the PCE infrastructure. As the applications of the PCE</p>																																																																																																																	
skipping to change at page 3, line 40		skipping to change at page 3, line 40																																																																																																																	
<p>Among the possible solutions mentioned in these documents, Transport Layer Security (TLS) [RFC5246] provides support for peer authentication, and message encryption and integrity. TLS supports the usage of well-known mechanisms to support key configuration and exchange, and means to perform security checks on the results of PCE discovery procedures via Interior Gateway Protocol (IGP) ([RFC5088] and [RFC5089]).</p>		<p>Among the possible solutions mentioned in these documents, Transport Layer Security (TLS) [RFC5246] provides support for peer authentication, and message encryption and integrity. TLS supports the usage of well-known mechanisms to support key configuration and exchange, and means to perform security checks on the results of PCE discovery procedures via Interior Gateway Protocol (IGP) ([RFC5088] and [RFC5089]).</p>																																																																																																																	

<p>This document describes a security container for the transport of PCEP messages, and therefore they do not affect the flexibility and extensibility of PCEP.</p> <p>This document describes how to apply TLS in securing PCE interactions, including initiation of the TLS procedures, the TLS handshake mechanisms, the TLS methods for peer authentication, the applicable TLS ciphersuites for data exchange, and the handling of errors in the security checks. In the rest of the document we will refer to this usage of TLS to provide a secure transport for PCEP as "PCEPS".</p>	<p>This document describes a security container for the transport of PCEP messages, and therefore it does not affect the flexibility and extensibility of PCEP.</p> <p>This document describes how to apply TLS in securing PCE interactions, including initiation of the TLS procedures, the TLS handshake mechanisms, the TLS methods for peer authentication, the applicable TLS ciphersuites for data exchange, and the handling of errors in the security checks. In the rest of the document we will refer to this usage of TLS to provide a secure transport for PCEP as "PCEPS".</p> <p>Within this document, PCEP communications are described through PCC-PCE relationship. The PCE architecture also supports the PCE-PCE communication, by having the requesting PCE fill the role of a PCC, as usual. Thus, the PCC refers to a PCC or a PCE initiating the PCEP session and acting as a client.</p>
<p>2. Requirements Language</p> <p>The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].</p> <p>3. Applying PCEPS</p> <p>3.1. Overview</p>	<p>2. Requirements Language</p> <p>The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].</p> <p>3. Applying PCEPS</p> <p>3.1. Overview</p>
<p>skipping to change at page 4, line 45</p>	
<p>3.2. Initiating the TLS Procedures</p> <p>Since PCEP can operate either with or without TLS, it is necessary for the PCEP speaker to indicate whether it wants to set up a TLS connection or not. For this purpose, this document specifies a new PCEP message called StartTLS. Thus the PCEP session is secured via TLS from the start before exchange of any other PCEP message (that includes the Open message). This document thus updates [RFC5440], which required the Open message to be the first PCEP message. In the case of a PCEP session using TLS the StartTLS message will be sent first.</p> <p>The PCEP speaker MAY discover that the PCEP peer supports PCEPS or can be preconfigured to use PCEPS for a given peer (see Section 4 for more details). Securing via TLS of an existing PCEP session is not permitted, the session MUST be closed and re-established with TLS as per the procedure described in this document.</p> <p>The StartTLS message is a PCEP message sent by a PCC to a PCE and by a PCE to a PCC in order to initiate the TLS procedure for PCEP. The Message-Type field of the PCEP common header for the StartTLS message</p>	<p>3.2. Initiating the TLS Procedures</p> <p>Since PCEP can operate either with or without TLS, it is necessary for the PCEP speaker to indicate whether it wants to set up a TLS connection or not. For this purpose, this document specifies a new PCEP message called StartTLS. Thus the PCEP session is secured via TLS from the start before exchange of any other PCEP message (that includes the Open message). This document thus updates [RFC5440], which required the Open message to be the first PCEP message. In the case of a PCEP session using TLS the StartTLS message will be sent first. Also a PCEP speaker that supports PCEPS MUST NOT start the OpenWait timer after the TCP establishment, instead it starts a StartTLSWait timer as described in Section 3.3.</p> <p>The PCEP speaker MAY discover that the PCEP peer supports PCEPS or can be preconfigured to use PCEPS for a given peer (see Section 4 for more details). Securing via TLS of an existing PCEP session is not permitted, the session MUST be closed and re-established with TLS as per the procedure described in this document.</p> <p>The StartTLS message is a PCEP message sent by a PCC to a PCE and by a PCE to a PCC in order to initiate the TLS procedure for PCEP. The Message-Type field of the PCEP common header for the StartTLS message</p>
<p>skipping to change at page 5, line 29</p>	
<p>StartTLS failure) and Error-value set to 1 (reception of StartTLS after any PCEP exchange), and MUST close the TCP connection. A PCEP speaker receiving any other message apart from StartTLS, Open, or PCErr as the first message, MUST treat it as an unexpected message and reply with a PCErr message with Error-Type set to [TBA2 by IANA] (PCEP StartTLS failure) and Error-value set to 2 (reception of any other message apart from StartTLS, Open, or PCErr message), and MUST close the TCP connection.</p> <p>If the PCEP speaker that does not support PCEPS, receives a StartTLS message, it MUST behave according to the existing error mechanism described in section 6.2 of [RFC5440] (in case message is received prior to an Open message) or section 6.9 of [RFC5440] (for the case of reception of unknown message).</p> <p>After the exchange of startTLS messages, if a PCEP speaker cannot</p> <p>establish a TLS connection for some reason (e.g. the required mechanisms for certificate revocation checking are not available), it MUST return a PCErr message (in clear) with Error-Type set to [TBA2 by IANA] (PCEP StartTLS failure) and Error-value set to:</p> <ul style="list-style-type: none"> o 3 (not without TLS) if it is not willing to exchange PCEP messages without the solicited TLS connection, and it MUST close the TCP session. o 4 (ok without TLS) if it is willing to exchange PCEP messages without the solicited TLS connection, and it MUST close the TCP 	<p>skipping to change at page 5, line 37</p> <p>StartTLS failure) and Error-value set to 1 (reception of StartTLS after any PCEP exchange), and MUST close the TCP connection. A PCEP speaker receiving any other message apart from StartTLS, Open, or PCErr as the first message, MUST treat it as an unexpected message and reply with a PCErr message with Error-Type set to [TBA2 by IANA] (PCEP StartTLS failure) and Error-value set to 2 (reception of any other message apart from StartTLS, Open, or PCErr message), and MUST close the TCP connection.</p> <p>If the PCEP speaker that does not support PCEPS, receives a StartTLS message, it will behave according to the existing error mechanism described in section 6.2 of [RFC5440] (in case message is received prior to an Open message) or section 6.9 of [RFC5440] (for the case of reception of unknown message). See Section 5 for more details.</p> <p>If the PCEP speaker that only supports PCEPS connection (as a local policy), receives an Open message, it MUST treat it as an unexpected message and reply with a PCErr message with Error-Type set to 1 (PCEP session establishment failure) and Error-value set to 1 (reception of an invalid Open message or a non Open message), and MUST close the TCP connection.</p> <p>If a PCC that supports PCEPS connection as well as allow non-PCEPS connection (as a local policy), it MUST first try to establish PCEPS, by sending StartTLS message and in case it receives a PCErr from the PCE, it MAY retry to establish connection without PCEPS by sending an Open message. If a PCE that supports PCEPS connection as well as allow non-PCEPS connection (as a local policy), it MUST wait to respond after TCP establishment, based on the message received from the PCC. In case of StartTLS message, PCE responds with sending StartTLS message and moving to TLS establishment procedures as described in this document. In case of Open message, PCE responds with Open message and move to PCEP session establishment procedure as per [RFC5440].</p> <p>After the exchange of StartTLS messages, if a PCEP speaker cannot establish a TLS connection for some reason (e.g. the required mechanisms for certificate revocation checking are not available), it MUST return a PCErr message (in clear) with Error-Type set to [TBA2 by IANA] (PCEP StartTLS failure) and Error-value set to:</p> <ul style="list-style-type: none"> o 3 (not without TLS) if it is not willing to exchange PCEP messages without the solicited TLS connection, and it MUST close the TCP session. o 4 (ok without TLS) if it is willing to exchange PCEP messages without the solicited TLS connection, and it MUST close the TCP

session. The peer MAY choose to re-establish the PCEP session without TLS next.

If the PCEP speaker supports PCEPS and can establish a TLS connection it MUST start the TLS connection establishment steps described in Section 3.4 before the PCEP initialization procedure (section 4.2.1 of [RFC5440]).

A PCEP speaker that does not support PCEPS or has learned the peer willingness to reestablish session without TLS, can send the Open message directly, as per [RFC5440].

session. The receiver MAY choose to re-establish the PCEP session without TLS next.

If the PCEP speaker supports PCEPS and can establish a TLS connection it MUST start the TLS connection establishment steps described in Section 3.4 before the PCEP initialization procedure (section 4.2.1 of [RFC5440]).

A PCEP speaker that does not support PCEPS or has learned the peer willingness to reestablish session without TLS, can send the Open message directly, as per [RFC5440].

skipping to change at page 6, line 48

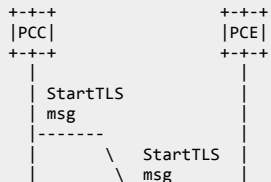
exchange of Open messages MUST be applied by the PCEP peers during the exchange of StartTLS messages.

The format of a StartTLS message is as follows:

<StartTLS Message>::= <Common Header>

The StartTLS message MUST contain only the PCEP common header with Message-Type field set to [TBA1 by IANA].

Once the TCP connection has been successfully established and the StartTLS message sent, the sender MUST start a timer called StartTLSWait timer, after the expiration of which, if no StartTLS message has been received, it MUST send a PCErr message and releases the TCP connection with Error-Type set to [TBA2 by IANA] and Error-value set to 5 (no StartTLS message received before the expiration of the StartTLSWait timer). A RECOMMENDED value for StartTLSWait timer is 60 seconds.



skipping to change at page 7, line 29

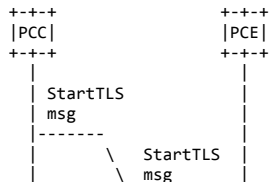
exchange of Open messages MUST be applied by the PCEP peers during the exchange of StartTLS messages.

The format of a StartTLS message is as follows:

<StartTLS Message>::= <Common Header>

The StartTLS message MUST contain only the PCEP common header with Message-Type field set to [TBA1 by IANA].

Once the TCP connection has been successfully established, the PCEP speaker MUST start a timer called StartTLSWait timer, after the expiration of which, if neither StartTLS message has been received, nor a PCErr/Open (in case of failure and PCEPS not supported by the peer respectively), it MUST send a PCErr message with Error-Type set to [TBA2 by IANA] and Error-value set to 5 (no StartTLS (nor PCErr/Open) message received before the expiration of the StartTLSWait timer) and it MUST release the TCP connection. A RECOMMENDED value for StartTLSWait timer is 60 seconds. The value of StartTLSWait timer MUST NOT be less than OpenWait timer.



skipping to change at page 7, line 32

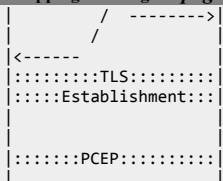


Figure 1: Both PCEP Speaker supports PCEPS

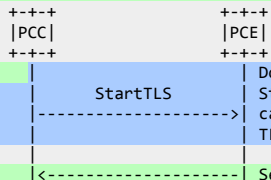
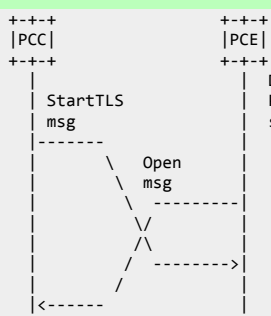


Figure 2: Both PCEP Speaker supports PCEPS, But cannot establish TLS



skipping to change at page 8, line 27

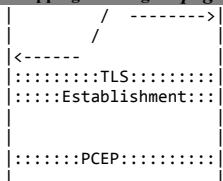


Figure 1: Both PCEP Speaker supports PCEPS (strict)

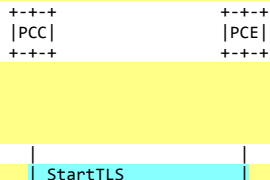
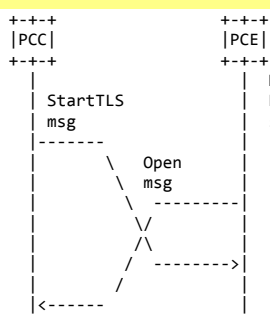


Figure 2: Both PCEP Speaker supports PCEPS (strict), but cannot establish TLS



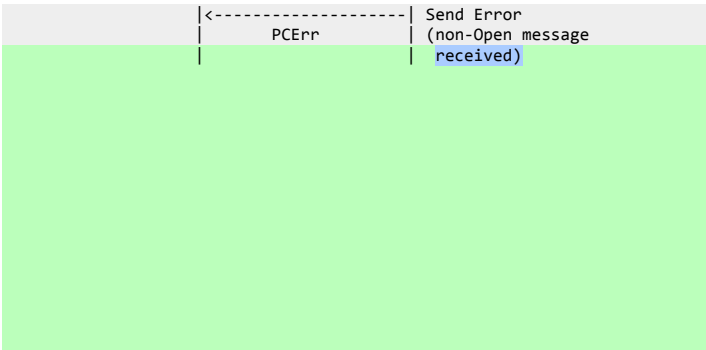


Figure 3: One PCEP Speaker does not support PCEPS

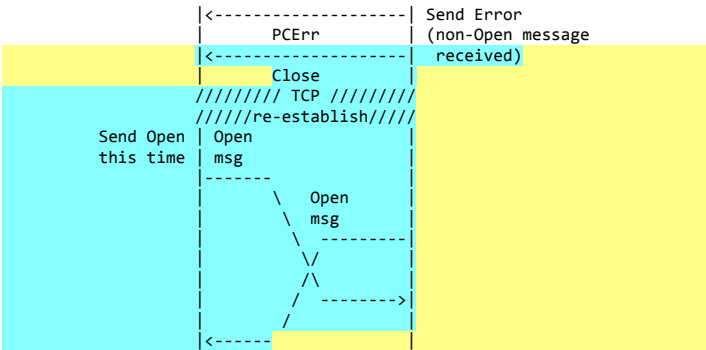


Figure 3: One PCEP Speaker (PCE) does not support PCEPS, while PCC supports both with or without PCEPS

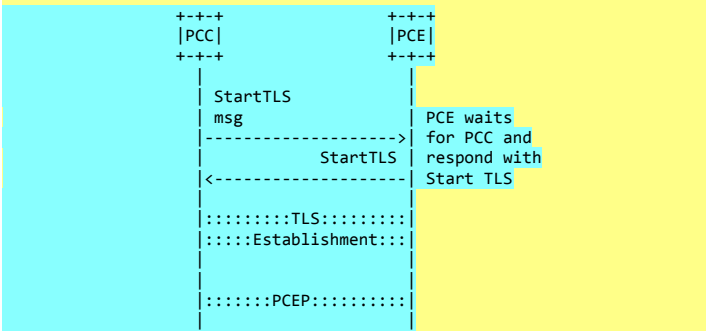


Figure 4: Both PCEP Speaker supports PCEPS as well as without PCEPS

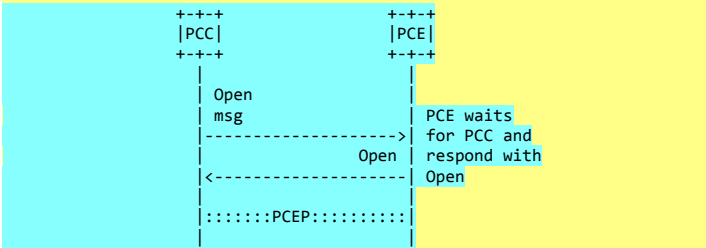


Figure 5: PCE supports PCEPS as well as without PCEPS, while PCC does not support PCEPS

3.4. TLS Connection Establishment

Once the establishment of TLS has been agreed by the PCEP peers, the connection establishment SHALL follow the following steps:

1. Immediately negotiate TLS sessions according to [RFC5246]. The following restrictions apply:
 - * Support for TLS v1.2 [RFC5246] or later is REQUIRED.
 - * Support for certificate-based mutual authentication is REQUIRED.
 - * Negotiation of mutual authentication is REQUIRED.
 - * Negotiation of a ciphersuite providing for integrity

skipping to change at page 10, line 11

- * TLS with X.509 certificates using certificate fingerprints: Implementations MUST allow the configuration of a list of trusted certificates, identified via fingerprint of the Distinguished Encoding Rules (DER) encoded certificate octets. Implementations MUST support SHA-256 as defined by [SHS] as the hash algorithm for the fingerprint.

3. Start exchanging PCEP messages.

To support TLS re-negotiation both peers MUST support the mechanism described in [RFC5746]. Any attempt to initiate a TLS handshake to establish new cryptographic parameters not aligned with [RFC5746] SHALL be considered a TLS negotiation failure.

3.5. Peer Identity

Depending on the peer authentication method in use, PCEPS supports different operation modes to establish peer's identity and whether it is entitled to perform requests or can be considered authoritative in

skipping to change at page 11, line 4

3.4. TLS Connection Establishment

Once the establishment of TLS has been agreed by the PCEP peers, the connection establishment SHALL follow the following steps:

1. Immediately negotiate a TLS session according to [RFC5246]. The following restrictions apply:
 - * Support for TLS v1.2 [RFC5246] or later is REQUIRED.
 - * Support for certificate-based mutual authentication is REQUIRED.
 - * Negotiation of mutual authentication is REQUIRED.
 - * Negotiation of a ciphersuite providing for integrity

skipping to change at page 13, line 22

- * TLS with X.509 certificates using certificate fingerprints: Implementations MUST allow the configuration of a list of trusted certificates, identified via fingerprint of the Distinguished Encoding Rules (DER) encoded certificate octets. Implementations MUST support SHA-256 as defined by [SHS] as the hash algorithm for the fingerprint.

3. Start exchanging PCEP messages.

- * Once the TLS connection has been successfully established, the PCEP speaker MUST start the OpenWait timer [RFC5440], after the expiration of which, if no Open message has been received, it sends a PCErr message and releases the TCP/TLS connection.

To support TLS re-negotiation both peers MUST support the mechanism described in [RFC5746]. Any attempt to initiate a TLS handshake to establish new cryptographic parameters not aligned with [RFC5746] SHALL be considered a TLS negotiation failure.

3.5. Peer Identity

Depending on the peer authentication method in use, PCEPS supports different operation modes to establish peer's identity and whether it is entitled to perform requests or can be considered authoritative in

skipping to change at page 14, line 19

31/07/2017Diff: draft-ietf-pce-pceps-14.txt - draft-ietf-pce-pceps-15.txt	
<ul style="list-style-type: none">o Peer's fully qualified domain name (FQDN)o Certificate Fingerprinto Issuero Subjecto All X509v3 Extended Key Usage	<ul style="list-style-type: none">o Peer's fully qualified domain name (FQDN)o Certificate Fingerprinto Issuero Subjecto All X509v3 Extended Key Usage
<ul style="list-style-type: none">o All X509v3 Subject Alternative Nameo All X509v3 Certificate Policies	<ul style="list-style-type: none">o All X509v3 Subject Alternative Nameo All X509v3 Certificate Policies
<p>[I-D.ietf-pce-stateful-sync-optimizations] specify a Speaker Entity Identifier TLV (SPEAKER-ENTITY-ID), as an optional TLV that MAY be included in the OPEN Object. It contains a unique identifier for the node that does not change during the lifetime of the PCEP speaker. An implementation would thus expose the speaker entity identifier as part of the X509v3 certificate, so that an implementation could use this identifier for the peer identification trust model.</p> <p>In addition, a PCC MAY apply the procedures described in [RFC6698] DNS-Based Authentication of Named Entities (DANE) to verify its peer</p>	<p>Note that the remote IP address used for the TCP session establishment is also exposed.</p> <p>[I-D.ietf-pce-stateful-sync-optimizations] specify a Speaker Entity Identifier TLV (SPEAKER-ENTITY-ID), as an optional TLV that MAY be included in the OPEN Object. It contains a unique identifier for the node that does not change during the lifetime of the PCEP speaker. An implementation would thus expose the speaker entity identifier as part of the X509v3 certificate, so that an implementation could use this identifier for the peer identification trust model.</p> <p>In addition, a PCC MAY apply the procedures described in [RFC6698] DNS-Based Authentication of Named Entities (DANE) to verify its peer</p>
skipping to change at page 11, line 32	skipping to change at page 15, line 7
<p>In case the initial TLS negotiation or the peer identity check fails, according to the procedures listed in this document, the peer MUST first send a PCERR message as per Section 3.2 and then terminate the session. It SHOULD follow the procedure listed in [RFC5440] to retry session setup along with an exponential back-off session establishment retry procedure.</p> <p>4. Discovery Mechanisms</p> <p>A PCE can advertise its capability to support PCEPS using the IGP advertisement and discovery mechanism. The PCE-CAP-FLAGS sub-TLV is an optional sub-TLV used to advertise PCE capabilities. It MAY be present within the PCE Discovery (PCED) sub-TLV carried by OSPF or IS-IS. [RFC5088] and [RFC5089] provide the description and processing rules for this sub-TLV when carried within OSPF and IS-IS, respectively. PCE capability bits are defined in [RFC5088]. A new capability flag bit for the PCE-CAP-FLAGS sub-TLV that can be announced as attribute to distribute PCEP security support information is proposed in [I-D.wu-pce-discovery-pceps-support]</p> <p>When DNS is used by a PCC (or a PCE acting as a client, for the rest of the section, PCC refers to both) willing to use PCEPS to locate an appropriate PCE [I-D.wu-pce-dns-pce-discovery], the PCC as an initiating entity, chooses at least one of the returned FQDNs to resolve, which it does by performing DNS "A" or "AAAA" lookups on the FQDN. This will eventually result in an IPv4 or IPv6 address. The PCC SHALL use the IP address(es) from the successfully resolved FQDN (with the corresponding port number returned by the DNS Service Record (SRV) lookup) as the connection address(es) for the receiving entity.</p> <p>If the PCC fails to connect using an IP address but the "A" or "AAAA" lookups returned more than one IP address, then the PCC SHOULD use the next resolved IP address for that FQDN as the connection address. If the PCC fails to connect using all resolved IP addresses for a given FQDN, then it SHOULD repeat the process of resolution and connection for the next FQDN returned by the SRV lookup based on the priority and weight.</p> <p>If the PCC receives a response to its SRV query but it is not able to establish a PCEPS connection using the data received in the response, as initiating entity it MAY fall back to lookup a PCE that uses TCP as transport.</p>	<p>In case the initial TLS negotiation or the peer identity check fails, according to the procedures listed in this document, the peer MUST first send a PCERR message as per Section 3.2 and then terminate the session. It SHOULD follow the procedure listed in [RFC5440] to retry session setup along with an exponential back-off session establishment retry procedure.</p> <p>4. Discovery Mechanisms</p> <p>This document does not specify any discovery mechanism for support of PCEPS. Other documents, [I-D.wu-pce-discovery-pceps-support] and [I-D.wu-pce-dns-pce-discovery] have made proposals:</p> <ul style="list-style-type: none">o A PCE can advertise its capability to support PCEPS using the IGP's advertisement mechanism of the PCE discovery information. The PCE-CAP-FLAGS sub-TLV is an optional sub-TLV used to advertise PCE capabilities. It is present within the PCE Discovery (PCED) sub-TLV carried by OSPF or IS-IS. [RFC5088] and [RFC5089] provide the description and processing rules for this sub-TLV when carried within OSPF and IS-IS, respectively. PCE capability bits are defined in [RFC5088]. A new capability flag bit for the PCE-CAP-FLAGS sub-TLV that can be announced as an attribute to distribute PCEP security support information is proposed in [I-D.wu-pce-discovery-pceps-support].o A PCE can advertise its capability to support PCEPS using the DNS [I-D.wu-pce-dns-pce-discovery] by identifying the support of TLS.
4.1. DANE Applicability	4.1. DANE Applicability
<p>DANE [RFC6698] defines a secure method to associate the certificate that is obtained from a TLS server with a domain name using DNS, i.e., using the TLSA DNS resource record (RR) to associate a TLS server certificate or public key with the domain name where the record is found, thus forming a "TLSA certificate association". The DNS information needs to be protected by DNS Security (DNSSEC). A PCC willing to apply DANE to verify server identity MUST conform to</p>	<p>DANE [RFC6698] defines a secure method to associate the certificate that is obtained from a TLS server with a domain name using DNS, i.e., using the TLSA DNS resource record (RR) to associate a TLS server certificate or public key with the domain name where the record is found, thus forming a "TLSA certificate association". The DNS information needs to be protected by DNS Security (DNSSEC). A PCC willing to apply DANE to verify server identity MUST conform to</p>
skipping to change at page 12, line 43	skipping to change at page 15, line 49
5. Backward Compatibility	5. Backward Compatibility
<p>The procedures described in this document define a security container for the transport of PCEP requests and replies carried by a TLS connection initiated by means of a specific extended message (StartTLS) that does not interfere with PCEP speaker implementations not supporting it.</p> <p>If a PCEP implementation that does not support PCEPS receives a StartTLS message, it would behave according to the existing error mechanism of [RFC5440].</p>	<p>The procedures described in this document define a security container for the transport of PCEP requests and replies carried by a TLS connection initiated by means of a specific extended message (StartTLS) that does not interfere with PCEP speaker implementations not supporting it.</p> <p>If a PCEP implementation that does not support PCEPS receives a StartTLS message, it would behave according to the existing error mechanism of [RFC5440]. On receiving the error, based on the local policy, a peer could try to establishing PCEP session without TLS as per the procedures defined in [RFC5440]. For successful TLS</p>

operations with PCEP, both PCEP peers in the network would need to be upgraded to support this document.

An existing PCEP session cannot be upgraded to PCEPS, the session needs to be terminated and reestablished as per the procedure described in this document. During the incremental upgrade, the PCEP speaker SHOULD allow session establishment with and without TLS. Once both PCEP speakers are upgraded to support PCEPS, the PCEP session is re-established with TLS, otherwise PCEP session without TLS is setup. A redundant PCE MAY also be used during the incremental deployment to take over the PCE undergoing upgrade. Once the upgrade is completed, support for unsecured version SHOULD be removed.

6. IANA Considerations

6.1. New PCEP Message

IANA is requested to allocate new message types within the "PCEP Messages" sub-registry of the PCEP Numbers registry, as follows:

Value	Description	Reference
TBA1	The Start TLS Message (StartTLS)	This document

6.2. New Error-Values

IANA is requested to allocate new Error Types and Error Values within the "PCEP-ERROR Object Error Types and Values" sub-registry of the PCEP Numbers registry, as follows:

Error-Type	Meaning	Error-value	Reference
TBA2	StartTLS Failure	0:Unassigned	This document
		1:Reception of StartTLS after any PCEP exchange	This document
		2:Reception of any other message apart from StartTLS, Open or PCErr	This document
		3:Failure, connection without TLS not possible	This document
		4:Failure, connection without TLS possible	This document
		5:No StartTLS message	This document
		before StartTLSWait timer expiry	

7. Security Considerations

While the application of TLS satisfies the requirement on privacy as well as fine-grained, policy-based peer authentication, there are security threats that it cannot address. It may be advisable to apply additional protection measures, in particular in what relates to attacks specifically addressed to forging the TCP connection

6. IANA Considerations

6.1. New PCEP Message

IANA is requested to allocate new message types within the "PCEP Messages" sub-registry of the PCEP Numbers registry, as follows:

Value	Description	Reference
TBA1	The Start TLS Message (StartTLS)	This document

6.2. New Error-Values

IANA is requested to allocate new Error Types and Error Values within the "PCEP-ERROR Object Error Types and Values" sub-registry of the PCEP Numbers registry, as follows:

Error-Type	Meaning	Error-value	Reference
TBA2	PCEP StartTLS failure	0:Unassigned	This document
		1:Reception of StartTLS after any PCEP exchange	This document
		2:Reception of any other message apart from StartTLS, Open or PCErr	This document
		3:Failure, connection without TLS not possible	This document
		4:Failure, connection without TLS possible	This document
		5:No StartTLS message (nor PCErr/Open)	This document
		before StartTLSWait timer expiry	

7. Security Considerations

While the application of TLS satisfies the requirement on privacy as well as fine-grained, policy-based peer authentication, there are security threats that it cannot address. It may be advisable to apply additional protection measures, in particular in what relates to attacks specifically addressed to forging the TCP connection

skipping to change at page 14, line 41

A PCE or PCC implementation MUST allow configuring the PCEP security via TLS capabilities as described in this document.

A PCE or PCC implementation supporting PCEP security via TLS MUST support general TLS configuration as per [RFC5246]. At least the configuration of one of the trust models and its corresponding parameters, as described in Section 3.4 and Section 3.5, MUST be supported by the implementation.

A PCEP implementation SHOULD allow configuring the following PCEP security parameters:

- o StartTLSWait timer value

PCEPS implementations MAY provide an option to allow the operator to manually override strict TLS configuration and allow unsecure connections. Execution of this override SHOULD trigger a warning about the security implications of permitting unsecure connections.

Further, the operator needs to develop suitable security policies around PCEP within his network. Further the PCEP peers SHOULD provide ways for the operator to complete the following tasks:

- o Determine if a PCEP session is protected via PCEPS.
- o Determine the version of TLS, the mechanism used for authentication, and the ciphersuite in use.
- o Determine if the certificate could not be verified, and the reason for this circumstance.
- o Inspect the certificate offered by the PCEP peer.
- o Be warned if StartTLS procedure fails for the PCEP peers, that are known to support PCEPS, via configurations or capability advertisements.

8.2. Information and Data Models

The PCEP MIB module SHOULD be extended to include PCEPS capabilities,

skipping to change at page 18, line 32

A PCE or PCC implementation MUST allow configuring the PCEP security via TLS capabilities as described in this document.

A PCE or PCC implementation supporting PCEP security via TLS MUST support general TLS configuration as per [RFC5246]. At least the configuration of one of the trust models and its corresponding parameters, as described in Section 3.4 and Section 3.5, MUST be supported by the implementation.

A PCEP implementation SHOULD allow configuring the StartTLSWait timer value.

PCEPS implementations MAY provide an option to allow the operator to manually override strict TLS configuration and allow unsecure connections. Execution of this override SHOULD trigger a warning about the security implications of permitting unsecure connections.

Further, the operator needs to develop suitable security policies around PCEP within his network. Further the PCEP peers SHOULD provide ways for the operator to complete the following tasks in regards to a PCEP session:

- o Determine if a session is protected via PCEPS.
- o Determine the version of TLS, the mechanism used for authentication, and the ciphersuite in use.
- o Determine if the certificate could not be verified, and the reason for this circumstance.
- o Inspect the certificate offered by the PCEP peer.
- o Be warned if StartTLS procedure fails for the PCEP peers, that are known to support PCEPS, via configurations or capability advertisements.

8.2. Information and Data Models

The PCEP MIB module is defined in [RFC7420]. The MIB module could be

information, and status.	extended to include the ability to view the PCEPS capability, TLS related information as well as TLS status for each PCEP peer.
An implementation SHOULD allow the operator to configure the PCEPS capability and various TLS related parameters, as well as allow to view the current TLS status for a PCEP session. To serve this purpose, the PCEP YANG module [I-D.ietf-pce-pcep-yang] can be extended to include TLS related configuration and state.	An implementation SHOULD also allow the operator to configure the PCEPS capability and various TLS related parameters in addition to ability to view the current TLS status for a PCEP session. To serve this purpose, the PCEP YANG module [I-D.ietf-pce-pcep-yang] is extended to include TLS related configuration and state information.
8.3. Liveness Detection and Monitoring	8.3. Liveness Detection and Monitoring
Mechanisms defined in this document do not imply any new liveness detection and monitoring requirements in addition to those already listed in [RFC5440] and [RFC5246].	Mechanisms defined in this document do not imply any new liveness detection and monitoring requirements in addition to those already listed in [RFC5440] and [RFC5246].
8.4. Verify Correct Operations	8.4. Verifying Correct Operations
A PCEPS implementation SHOULD log error events and provide PCEPS failure statistics with reasons.	A PCEPS implementation SHOULD log error events and provide PCEPS failure statistics with reasons.
8.5. Requirements on Other Protocols	8.5. Requirements on Other Protocols
Mechanisms defined in this document do not imply any new requirements on other protocols.	Mechanisms defined in this document do not imply any new requirements on other protocols. Note that, Section 4 list possible discovery mechanism for support of PCEPS.
8.6. Impact on Network Operation	8.6. Impact on Network Operation
Mechanisms defined in this document do not have any significant impact on network operations in addition to those already listed in [RFC5440], and the policy and management implications discussed above.	Mechanisms defined in this document do not have any significant impact on network operations in addition to those already listed in [RFC5440], and the policy and management implications discussed above.
9. Acknowledgements	9. Acknowledgements
This specification relies on the analysis and profiling of TLS included in [RFC6614] and the procedures described for the STARTTLS command in [RFC4513].	This specification relies on the analysis and profiling of TLS included in [RFC6614] and the procedures described for the STARTTLS command in [RFC4513].
We would like to thank Joe Touch for his suggestions and support regarding the TLS start mechanisms.	We would like to thank Joe Touch for his suggestions and support regarding the TLS start mechanisms.
Thanks to Dan King for reminding the authors about manageability considerations.	Thanks to Daniel King for reminding the authors about manageability considerations.
Thanks to Cyril Margaria for shepherding this document.	Thanks to Cyril Margaria for shepherding this document.
Thanks to Dan Frost for the RTGDIR review.	Thanks to David Mandelberg for early SECDIR review comments as well as re-reviewing during IETF last call.
	Thanks to Dan Frost for the RTGDIR review and comments.
	Thanks to Dale Worley for the Gen-ART review and comments.
	Also thanks to Tianran Zhou for OPSDIR review.
	Thanks to Deborah Brungard for being the responsible AD and guiding the authors as needed.
10. References	10. References
10.1. Normative References	10.1. 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, <http://www.rfc-editor.org/info/rfc2119>.	[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.
skipping to change at page 18, line 20	
"Transport Layer Security (TLS) Encryption for RADIUS", RFC 6614, DOI 10.17487/RFC6614, May 2012, <http://www.rfc-editor.org/info/rfc6614>.	"Transport Layer Security (TLS) Encryption for RADIUS", RFC 6614, DOI 10.17487/RFC6614, May 2012, <http://www.rfc-editor.org/info/rfc6614>.
[RFC6952] Jethanandani, M., Patel, K., and L. Zheng, "Analysis of BGP, LDP, PCEP, and MSDP Issues According to the Keying and Authentication for Routing Protocols (KARP) Design Guide", RFC 6952, DOI 10.17487/RFC6952, May 2013, <http://www.rfc-editor.org/info/rfc6952>.	[RFC6952] Jethanandani, M., Patel, K., and L. Zheng, "Analysis of BGP, LDP, PCEP, and MSDP Issues According to the Keying and Authentication for Routing Protocols (KARP) Design Guide", RFC 6952, DOI 10.17487/RFC6952, May 2013, <http://www.rfc-editor.org/info/rfc6952>.
	[RFC7420] Koushik, A., Stephan, E., Zhao, Q., King, D., and J. Hardwick, "Path Computation Element Communication Protocol (PCEP) Management Information Base (MIB) Module", RFC 7420, DOI 10.17487/RFC7420, December 2014, <http://www.rfc-editor.org/info/rfc7420>.
[I-D.ietf-pce-stateful-sync-optimizations] Crabbe, E., Minei, I., Medved, J., Varga, R., Zhang, X., and D. Dhody, "Optimizations of Label Switched Path State Synchronization Procedures for a Stateful PCE", draft-ietf-pce-stateful-sync-optimizations-10 (work in progress), March 2017.	[I-D.ietf-pce-stateful-sync-optimizations] Crabbe, E., Minei, I., Medved, J., Varga, R., Zhang, X., and D. Dhody, "Optimizations of Label Switched Path State Synchronization Procedures for a Stateful PCE", draft-ietf-pce-stateful-sync-optimizations-10 (work in progress), March 2017.
[I-D.ietf-pce-pcep-yang] Dhody, D., Hardwick, J., Beeram, V., and j. jeffrant@gmail.com, "A YANG Data Model for Path Computation Element Communications Protocol (PCEP)", draft-ietf-pce-pcep-yang-02 (work in progress), March 2017.	[I-D.ietf-pce-pcep-yang] Dhody, D., Hardwick, J., Beeram, V., and j. jeffrant@gmail.com, "A YANG Data Model for Path Computation Element Communications Protocol (PCEP)", draft-ietf-pce-pcep-yang-05 (work in progress), June 2017.
[I-D.wu-pce-dns-pce-discovery] Wu, Q., Dhody, D., King, D., Lopez, D., and J. Tantsura,	[I-D.wu-pce-dns-pce-discovery] Wu, Q., Dhody, D., King, D., Lopez, D., and J. Tantsura,

<div>"Path Computation Element (PCE) Discovery using Domain Name System(DNS)", draft-wu-pce-dns-pce-discovery-10 (work in progress), March 2017.</div> <div>[I-D.wu-pce-discovery-pceps-support] Lopez, D., Wu, Q., Dhody, D., and D. King, "IGP extension for PCEP security capability support in the PCE</div>	<div>"Path Computation Element (PCE) Discovery using Domain Name System(DNS)", draft-wu-pce-dns-pce-discovery-10 (work in progress), March 2017.</div> <div>[I-D.wu-pce-discovery-pceps-support] Lopez, D., Wu, Q., Dhody, D., and D. King, "IGP extension for PCEP security capability support in the PCE</div>
End of changes. 40 change blocks.	
106 lines changed or deleted	222 lines changed or added

This html diff was produced by rfcdiff 1.45. The latest version is available from <http://tools.ietf.org/tools/rfcdiff/>