RFC 9353
IGP Extension for Path Computation Element Communication Protocol (PCEP) Security Capability Support in PCE Discovery (PCED)

Abstract

When a Path Computation Element (PCE) is a Label Switching Router (LSR) or a server participating in the Interior Gateway Protocol (IGP), its presence and path computation capabilities can be advertised using IGP flooding. The IGP extensions for PCE Discovery (PCED) (RFCs 5088 and 5089) define a method to advertise path computation capabilities using IGP flooding for OSPF and IS-IS, respectively. However, these specifications lack a method to advertise Path Computation Element Communication Protocol (PCEP) security (e.g., Transport Layer Security (TLS) and TCP Authentication Option (TCP-AO)) support capability.

This document defines capability flag bits for the PCE-CAP-FLAGS sub-TLV that can be announced as an attribute in the IGP advertisement to distribute PCEP security support information. In addition, this document updates RFCs 5088 and 5089 to allow advertisement of a Key ID or KEY-CHAIN-NAME sub-TLV to support TCP-AO security capability. This document also updates RFCs 8231 and 8306.

Status of This Memo

This is an Internet Standards Track document.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Further information on Internet Standards is available in Section 2 of RFC 7841.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at https://www.rfc-editor.org/info/rfc9353.
Copyright Notice

Copyright (c) 2023 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 Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction
2. Conventions Used in This Document
3. IGP Extension for PCEP Security Capability Support
   3.1. Use of PCEP Security Capability Support for PCED
   3.2. KEY-ID Sub-TLV
       3.2.1. IS-IS
       3.2.2. OSPF
   3.3. KEY-CHAIN-NAME Sub-TLV
       3.3.1. IS-IS
       3.3.2. OSPF
4. Updates to RFCs
5. Backward Compatibility Considerations
6. Management Considerations
   6.1. Control of Policy and Functions
   6.2. Information and Data Model
   6.3. Liveness Detection and Monitoring
   6.4. Verification of Correct Operations
   6.5. Requirements on Other Protocols and Functional Components
   6.6. Impact on Network Operations
7. Security Considerations
1. Introduction

As described in [RFC5440], privacy and integrity are important issues for communication using the Path Computation Element Communication Protocol (PCEP); an attacker that intercepts a PCEP message could obtain sensitive information related to computed paths and resources. Authentication and integrity checks allow the receiver of a PCEP message to know that the message genuinely comes from the node that purports to have sent it and whether the message has been modified.

Among the possible solutions mentioned in [RFC5440], Transport Layer Security (TLS) [RFC8446] provides support for peer authentication, message encryption, and integrity while TCP-AO [RFC5925] and Cryptographic Algorithms for TCP-AO [RFC5926] offer significantly improved security for applications using TCP. As specified in Section 4 of [RFC8253], the PCC needs to know whether the PCE server supports TLS or TCP-AO as a secure transport in order for a Path Computation Client (PCC) to establish a connection with a PCE server using TLS or TCP-AO.

[RFC5088] and [RFC5089] define a method to advertise path computation capabilities using IGP flooding for OSPF and IS-IS, respectively. However, these specifications lack a method to advertise PCEP security (e.g., TLS and TCP-AO) support capability.

This document defines capability flag bits for the PCE-CAP-FLAGS sub-TLV that can be announced as attributes in the IGP advertisement to distribute PCEP security support information. In addition, this document updates [RFC5088] and [RFC5089] to allow advertisement of a KeyID or KEY-CHAIN-NAME sub-TLV to support TCP-AO security capability.

IANA created a top-level registry titled "Path Computation Element (PCE) Capability Flags" per [RFC5088]. This document updates [RFC5088] and moves it to follow the heading of the "Interior Gateway Protocol (IGP) Parameters" registry. [RFC5089] states that the IS-IS PCE-CAP-FLAGS sub-TLV uses the same registry as OSPF. This document updates [RFC5089] to refer to the new IGP registry. Further, this document updates [RFC8231] where it references the registry location as the "Open Shortest Path First v2 (OSPFv2) Parameters" registry to the "Interior Gateway Protocol
Conventions Used in This Document

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.

IGP Extension for PCEP Security Capability Support

[RFC5088] defines a PCE Discovery (PCED) TLV carried in an OSPF Router Information Link State Advertisement (LSA) as defined in [RFC7770] to facilitate PCED using OSPF. This document defines two capability flag bits in the OSPF PCE Capability Flags to indicate TCP-AO support [RFC5925] [RFC5926] and PCEP over TLS support [RFC8253], respectively.

Similarly, [RFC5089] defines the PCED sub-TLV for use in PCED using IS-IS. This document will use the same flag for the OSPF PCE Capability Flags sub-TLV to allow IS-IS to indicate TCP-AO support and PCEP over TLS support, respectively.

The IANA assignments for shared OSPF and IS-IS Security Capability Flags are documented in Section 8.1 of this document.

Use of PCEP Security Capability Support for PCED

TCP-AO and PCEP over TLS support flag bits are advertised using IGP flooding.

- PCE supports TCP-AO: IGP advertisement SHOULD include a TCP-AO support flag bit.
- PCE supports TLS: IGP advertisement SHOULD include PCEP over TLS support flag bit.

If the PCE supports multiple security mechanisms, it SHOULD include all corresponding flag bits in its IGP advertisement.

Note that [RFC5557] uses the term "OSPF registry" instead of the "IGP registry", whereas [RFC8623] and [RFC9168] use the term "OSPF Parameters" instead of "IGP Parameters".

Note that the PCEP Open message exchange is another way to discover PCE capabilities information; however, in this instance, the TCP-security-related key parameters need to be known before the PCEP session is established and the PCEP Open messages are exchanged. Thus, the IGP advertisement and flooding mechanisms need to be leveraged for PCE discovery and capabilities advertisement.
A client's configuration MAY indicate that support for a given security capability is required. If a client is configured to require that its PCE server supports TCP-AO, the client MUST verify that the TCP-AO flag bit in the PCE-CAP-FLAGS sub-TLV for a given server is set before it opens a connection to that server. Similarly, if the client is configured to require that its PCE server supports TLS, the client MUST verify that the PCEP over TLS support flag bit in the PCE-CAP-FLAGS sub-TLV for a given server is set before it opens a connection to that server.

3.2. KEY-ID Sub-TLV

The KEY-ID sub-TLV specifies an identifier that can be used by the PCC to identify the TCP-AO key (referred to as "KeyID" in [RFC5925]).

3.2.1. IS-IS

The KEY-ID sub-TLV MAY be present in the PCED sub-TLV carried within the IS-IS Router CAPABILITY TLV when the capability flag bit of the PCE-CAP-FLAGS sub-TLV in IS-IS is set to indicate TCP-AO support.

The KEY-ID sub-TLV has the following format:

Type: 6
Length: 1
KeyID: The one-octet KeyID as per [RFC5925] to uniquely identify the Master Key Tuple (MKT).

3.2.2. OSPF

Similarly, this sub-TLV MAY be present in the PCED TLV carried within the OSPF Router Information LSA when the capability flag bit of the PCE-CAP-FLAGS sub-TLV in OSPF is set to indicate TCP-AO support.

The format of the KEY-ID sub-TLV is as follows:

```
+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+
| Type          | Length        | KeyID         | Reserved      |
+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+
| 000000000000  | 000000000000  | 000000000000  | 000000000000  |
+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+---------------+
```

Type: 6
Length: 4
KeyID: The one octet KeyID as per [RFC5925] to uniquely identify the MKT.
Reserved: MUST be set to zero while sending and ignored on receipt.
3.3. **KEY-CHAIN-NAME Sub-TLV**

The KEY-CHAIN-NAME sub-TLV specifies a key chain name that can be used by the PCC to identify the key chain. The key chain name could be manually configured via command-line interface (CLI) or installed in the YANG datastore (see [RFC8177]) at the PCC.

### 3.3.1. IS-IS

The KEY-CHAIN-NAME sub-TLV may be present in the PCED sub-TLV carried within the IS-IS Router CAPABILITY TLV when the capability flag bit of the PCE-CAP-FLAGS sub-TLV in IS-IS is set to indicate TCP-AO support.

The KEY-CHAIN-NAME sub-TLV has the following format:

**Type:** 7  
**Length:** Variable, encodes the length of the value field.  
**Key Chain Name:** The Key Chain Name contains a string of 1 to 255 octets to be used to identify the key chain. It **MUST** be encoded using UTF-8. A receiving entity **MUST NOT** interpret invalid UTF-8 sequences and ignore them. This field is not NULL terminated. UTF-8 “Shortest Form” encoding is **REQUIRED** to guard against the technical issues outlined in [UTR36].

### 3.3.2. OSPF

Similarly, this sub-TLV may be present in the PCED TLV carried within the OSPF Router Information LSA when the capability flag bit of the PCE-CAP-FLAGS sub-TLV in OSPF is set to indicate TCP-AO support. The sub-TLV **MUST** be zero-padded so that the sub-TLV is 4-octet aligned.

The format of KEY-CHAIN-NAME sub-TLV is as follows:

```
+---------------------------------+---------------------------------+  
|              Type = 7         |             Length            |  
+---------------------------------+---------------------------------+  
| //                     Key Chain Name                          |  
|                                                              |  
+---------------------------------+---------------------------------+  
```

**Type:** 7  
**Length:** Variable, padding is not included in the Length field.
Key Chain Name: The Key Chain Name contains a string of 1 to 255 octets to be used to identify the key chain. It MUST be encoded using UTF-8. A receiving entity MUST NOT interpret invalid UTF-8 sequences and ignore them. This field is not NULL terminated. UTF-8 “Shortest Form” encoding is REQUIRED to guard against the technical issues outlined in [UTR36]. The sub-TLV MUST be zero-padded so that the sub-TLV is 4-octet aligned.

4. Updates to RFCs

Section 4 of [RFC5088] states that no new sub-TLVs will be added to the PCED TLV and no new PCE information will be carried in the Router Information LSA. This document updates [RFC5088] by allowing the two sub-TLVs defined in this document to be carried in the PCED TLV advertised in the Router Information LSA.

Section 4 of [RFC5089] states that no new sub-TLVs will be added to the PCED TLV and no new PCE information will be carried in the Router CAPABILITY TLV. This document updates [RFC5089] by allowing the two sub-TLVs defined in this document to be carried in the PCED TLV advertised in the Router CAPABILITY TLV.

This introduction of additional sub-TLVs should be viewed as an exception to the policies in [RFC5088] and [RFC5089], which is justified by the requirement to discover the PCEP security support prior to establishing a PCEP session. The restrictions defined in [RFC5088] and [RFC5089] should still be considered to be in place. If new advertisements are required in the future, alternative mechanisms such as using [RFC6823] or [LSR-OSPF-TRANSPORT-INSTANCE] should be considered.

The registry for the PCE Capability Flags assigned in Section 8.3 of [RFC5557], Section 8.1 of [RFC8231], Section 6.9 of [RFC8306], Section 11.1 of [RFC8623], and Section 10.5 of [RFC9168] has changed to the IGP Parameters "Path Computation Element (PCE) Capability Flags" registry created in this document.

5. Backward Compatibility Considerations

An LSR that does not support the IGP PCE capability bits specified in this document silently ignores those bits.

An LSR that does not support the KEY-ID and KEY-CHAIN-NAME sub-TLVs specified in this document silently ignores those sub-TLVs.

IGP extensions defined in this document do not introduce any new interoperability issues.

6. Management Considerations

Manageability considerations for PCED are addressed in Section 4.10 of [RFC4674], Section 9 of [RFC5088], and Section 9 of [RFC5089].
6.1. Control of Policy and Functions

A PCE implementation SHOULD allow the following parameters to be configured on the PCE:

- support for TCP-AO
- the KeyID used by TCP-AO
- Key Chain Name
- support for TLS

6.2. Information and Data Model

The YANG module for PCEP [PCE-PCEP-YANG] supports PCEP security parameters (key, key chain, and TLS).

6.3. Liveness Detection and Monitoring

Normal operations of the IGP meet the requirements for liveness detection and monitoring.

6.4. Verification of Correct Operations

The correlation of PCEP security information advertised against information received can be achieved by comparing the information in the PCED sub-TLV received by the PCC with that stored at the PCE using the PCEP YANG.

6.5. Requirements on Other Protocols and Functional Components

There are no new requirements on other protocols.

6.6. Impact on Network Operations

Frequent changes in PCEP security information advertised in the PCED sub-TLV may have a significant impact on IGP and might destabilize the operation of the network by causing the PCCs to reconnect sessions with PCEs. Section 4.10.4 of [RFC4674], Section 9.6 of [RFC5088], and Section 9.6 of [RFC5089] list techniques that are applicable to this document as well.

7. Security Considerations

Security considerations as specified by [RFC5088] and [RFC5089] are applicable to this document.

As described in Section 10.2 of [RFC5440], a PCEP speaker MUST support TCP MD5 [RFC2385], so no capability advertisement is needed to indicate support. However, as noted in [RFC6952], TCP MD5 has been obsoleted by TCP-AO [RFC5925] because of security concerns. TCP-AO is not widely implemented; therefore, it is RECOMMENDED that PCEP be secured using TLS per [RFC8253] (which updates [RFC5440]). An implementation SHOULD offer at least one of the two security capabilities defined in this document.
The information related to PCEP security is sensitive and due care needs to be taken by the 
operator. This document defines new capability bits that are susceptible to a downgrade attack 
by setting them to zero. The content of the Key-ID or KEY-CHAIN-NAME sub-TLV can be altered to 
enable an on-path attack. Thus, before advertising the PCEP security parameters by using the 
mechanism described in this document, the IGP **MUST** be known to provide authentication and 
integrity for the PCED TLV using the mechanisms defined in [RFC5304], [RFC5310], or [RFC5709].

Moreover, as stated in the security considerations of [RFC5088] and [RFC5089], there are no 
mechanisms defined in OSPF or IS-IS to protect the confidentiality of the PCED TLV. For this 
reason, the operator must ensure that no private data is carried in the TLV. For example, the 
operator must ensure that KeyIDs or key chain names do not reveal sensitive information about 
the network.

### 8. IANA Considerations

#### 8.1. PCE Capability Flags

IANA has moved the "Path Computation Element (PCE) Capability Flags" registry from the "Open 
Shortest Path First v2 (OSPFv2) Parameters" grouping to the "Interior Gateway Protocol (IGP) 
Parameters" grouping.

IANA has made the following additional assignments from the "Path Computation Element (PCE) 
Capability Flags" registry:

<table>
<thead>
<tr>
<th>Bit</th>
<th>Capability Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>TCP-AO Support</td>
<td>RFC 9353</td>
</tr>
<tr>
<td>18</td>
<td>PCEP over TLS support</td>
<td>RFC 9353</td>
</tr>
</tbody>
</table>

*Table 1: Path Computation Element (PCE) Capability Flags Registrations*

The grouping is located at: [https://www.iana.org/assignments/igp-parameters/](https://www.iana.org/assignments/igp-parameters/).

#### 8.2. PCED Sub-TLV Type Indicators

The PCED sub-TLVs are defined in [RFC5088] and [RFC5089], but a corresponding IANA registry 
was not created. IANA has created a new registry called "PCE Discovery (PCED) Sub-TLV Type 
Indicators" under the "Interior Gateway Protocol (IGP) Parameters" registry. The registration 
policy for this registry is "Standards Action" [RFC8126]. Values in this registry come from the 
range 0-65535.

This registry is initially populated as follows:
This registry is used by both the OSPF PCED TLV and the IS-IS PCED sub-TLV.

This grouping is located at: <https://www.iana.org/assignments/igp-parameters/>.

9. References

9.1. Normative References


<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Reserved</td>
<td>RFC 9353, RFC 5088</td>
</tr>
<tr>
<td>1</td>
<td>PCE-ADDRESS</td>
<td>RFC 9353, RFC 5088</td>
</tr>
<tr>
<td>2</td>
<td>PATH-SCOPE</td>
<td>RFC 9353, RFC 5088</td>
</tr>
<tr>
<td>3</td>
<td>PCE-DOMAIN</td>
<td>RFC 9353, RFC 5088</td>
</tr>
<tr>
<td>4</td>
<td>NEIG-PCE-DOMAIN</td>
<td>RFC 9353, RFC 5088</td>
</tr>
<tr>
<td>5</td>
<td>PCE-CAP-FLAGS</td>
<td>RFC 9353, RFC 5088</td>
</tr>
<tr>
<td>6</td>
<td>KEY-ID</td>
<td>RFC 9353</td>
</tr>
<tr>
<td>7</td>
<td>KEY-CHAIN-NAME</td>
<td>RFC 9353</td>
</tr>
</tbody>
</table>

Table 2: Initial Contents of the PCED Sub-TLV Type Indicators Registry


9.2. Informative References


Acknowledgments

The authors of this document would like to thank Acee Lindem, Julien Meuric, Les Ginsberg, Ketan Talaulikar, Tom Petch, Aijun Wang, and Adrian Farrel for the review and comments.
The authors would also like to give special thanks to Michale Wang for his major contributions to the initial draft version.

Thanks to John Scudder for providing an excellent AD review. Thanks to Carlos Pignataro, Yaron Sheffer, Ron Bonica, and Will (Shucheng) LIU for directorate reviews.

Thanks to Lars Eggert, Robert Wilton, Roman Danyliw, Éric Vyncke, Paul Wouters, Murray Kucherawy, and Warren Kumari for IESG reviews.

Authors' Addresses

Diego R. Lopez
Telefonica I+D
Spain
Email: diego.r.lopez@telefonica.com

Qin Wu
Huawei Technologies
Yuhua District
101 Software Avenue
Nanjing
Jiangsu, 210012
China
Email: bill.wu@huawei.com

Dhruv Dhody
Huawei Technologies
Divyashree Techno Park, Whitefield
Bangalore 560037
Karnataka
India
Email: dhruv.ietf@gmail.com

Qiufang Ma
Huawei Technologies
Yuhua District
101 Software Avenue
Nanjing
Jiangsu, 210012
China
Email: maqiufang1@huawei.com

Daniel King
Old Dog Consulting
United Kingdom
Email: daniel@olddog.co.uk