

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: January 22, 2015

M. Wasserman
S. Hartman
Painless Security
D. Zhang
Huawei
July 21, 2014

Port Control Protocol (PCP) Authentication Mechanism
draft-ietf-pcp-authentication-04

Abstract

An IPv4 or IPv6 host can use the Port Control Protocol (PCP) to flexibly manage the IP address and port mapping information on Network Address Translators (NATs) or firewalls, to facilitate communications with remote hosts. However, the un-controlled generation or deletion of IP address mappings on such network devices may cause security risks and should be avoided. In some cases the client may need to prove that it is authorized to modify, create or delete PCP mappings. This document proposes an in-band authentication mechanism for PCP that can be used in those cases. The Extensible Authentication Protocol (EAP) is used to perform authentication between PCP devices.

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 <http://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 January 22, 2015.

Copyright Notice

Copyright (c) 2014 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 (<http://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.

Table of Contents

1.	Introduction	3
2.	Terminology	4
3.	Protocol Details	5
3.1.	Session Initiation	5
3.2.	Session Termination	8
3.3.	Session Re-Authentication	8
4.	PA Security Association	9
5.	Result Code	10
6.	Packet Format	10
6.1.	Packet Format of PCP Auth Messages	10
6.2.	Authentication OpCode	11
6.3.	Nonce Option	12
6.4.	Authentication Tag Option for Common PCP	12
6.5.	Authentication Tag Option for PCP Auth Messages	14
6.6.	EAP Payload Option	14
6.7.	PRF Option	15
6.8.	MAC Algorithm Option	15
6.9.	Session Lifetime Option	16
6.10.	Received Packet Option	16
6.11.	ID Indication Option	16
7.	Processing Rules	17
7.1.	Authentication Data Generation	17
7.2.	Authentication Data Validation	18
7.3.	Retransmission Policies for PCP Auth Messages	18
7.4.	Sequence Numbers for PCP Auth Messages	19
7.5.	Sequence Numbers for Common PCP Messages	20
7.6.	MTU Considerations	21
8.	IANA Considerations	21
9.	Security Considerations	21
10.	Acknowledgements	22
11.	Change Log	22
11.1.	Changes from wasserman-pcp-authentication-02 to ietf-pcp-authentication-00	22
11.2.	Changes from wasserman-pcp-authentication-01 to -02	22
11.3.	Changes from ietf-pcp-authentication-00 to -01	22
11.4.	Changes from ietf-pcp-authentication-01 to -02	22

11.5.	Changes from ietf-pcp-authentication-02 to -03	23
11.6.	Changes from ietf-pcp-authentication-03 to -04	23
12.	References	23
12.1.	Normative References	23
12.2.	Informative References	23
Authors' Addresses	24

[1.](#) Introduction

Using the Port Control Protocol (PCP) [[RFC6887](#)], an IPv4 or IPv6 host can flexibly manage the IP address mapping information on its network address translators (NATs) and firewalls, and control their policies in processing incoming and outgoing IP packets. Because NATs and firewalls both play important roles in network security architectures, there are many situations in which authentication and access control are required to prevent un-authorized users from accessing such devices. This document proposes a PCP security extension which enables PCP servers to authenticate their clients with Extensible Authentication Protocol (EAP). The EAP messages are encapsulated within PCP packets during transportation.

The following issues are considered in the design of this extension:

- o Loss of EAP messages during transportation
- o Disordered delivery of EAP messages
- o Generation of transport keys
- o Integrity protection and data origin authentication for PCP messages
- o Algorithm agility

The mechanism described in this document meets the security requirements to address the Advanced Threat Model described in the base PCP specification [[RFC6887](#)]. This mechanism can be used to secure PCP in the following situations::

- o On security infrastructure equipment, such as corporate firewalls, that does not create implicit mappings.
- o On equipment (such as CGNs or service provider firewalls) that serve multiple administrative domains and do not have a mechanism to securely partition traffic from those domains.

- o For any implementation that wants to be more permissive in authorizing explicit mappings than it is in authorizing implicit mappings.
- o For implementations that support the THIRD_PARTY Option (unless they can meet the constraints outlined in [Section 14.1.2.2](#)).
- o For implementations that wish to support any deployment scenario that does not meet the constraints described in [Section 14.1](#).

2. Terminology

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 [RFC 2119](#) [[RFC2119](#)].

Most of the terms used in this document are introduced in [[RFC6887](#)].

PCP Client: A PCP device (e.g., a host) which is responsible for issuing PCP requests to a PCP server. In this document, a PCP client is also a EAP peer [[RFC3748](#)], and it is the responsibility of a PCP client to provide the credentials when authentication is required.

PCP Server: A PCP device (e.g., a NAT or a firewall) that implements the server-side of the PCP protocol, via which PCP clients request and manage explicit mappings. In this document, a PCP server is integrated with an EAP authenticator [[RFC3748](#)]. Therefore, when necessary, a PCP server can verify the credentials provided by a PCP client and make an access control decision based on the authentication result.

PCP-Authentication (PA) Session: A series of PCP message exchanges transferred between a PCP client and a PCP server. The PCP message involved within a session includes the PA messages used to perform EAP authentication, key distribution and session management, and the common PCP messages secured with the keys distributed during authentication. Each PA session is assigned a distinctive Session ID.

Session Partner: A PCP device involved within a PA session. Each PA session has two session partners (a PCP server and a PCP client).

Session Lifetime: The life period associated with a PA session, which decides the lifetime of the current authorization given to the PCP client.

PCP Security Association (PCP SA): A PCP security association is formed between a PCP client and a PCP server by sharing cryptographic

keying material and associated context. The formed duplex security association is used to protect the bidirectional PCP signaling traffic between the PCP client and PCP server.

Master Session Key (MSK): A key derived by the partners of a PA session, using an EAP key generating method (e.g., the one defined in [\[RFC5448\]](#)).

PCP-Authentication (PA) message: A PCP message containing an Authentication OpCode. Particularly, a PA message sent from a PCP server to a PCP client is referred to as a PA-Server, while PA message sent from a PCP client to a PCP server is referred to as a PA-Client. Therefore, a PA-Server is actually a PCP response message specified in [\[RFC6887\]](#), and a PA-Client is a PCP request message. This document specifies an option, the Authentication Tag Option for PCP Auth, to provide integrity protection and message origin authentication for PA messages.

Common PCP message: A PCP message which does not contain an Authentication OpCode. This document specifies an option, the Authentication Tag Option for Common PCP, to provide integrity protection and message origin authentication for the common PCP messages.

3. Protocol Details

3.1. Session Initiation

At the beginning of a PA session, a PCP client and a PCP server need to exchange a series of PA messages in order to perform an EAP authentication process. Each PA message is attached with an Authentication OpCode and may optionally contain a set of Options for various purposes (e.g., transporting authentication messages and session managements). The Authentication OpCode consists of two fields: Session ID and Sequence Number. The Session ID field is used to identify the session to which the message belongs. The sequence number field is used to detect the disorder or the duplication occurred during packet delivery.

When a PCP client intends to proactively initiate a PA session with a PCP server, it sends a PA-Initiation message (a PA-Client message with the result code "INITIATION") to the PCP server. In the message, the Session ID and Sequence Number fields of the Authentication OpCode are set as 0. The PCP client MAY also optionally append a nonce option which consists of a random nonce with the message.

After receiving the PA-Initiation, if the PCP server agrees to initiate a PA session with the PCP client, it will reply with a PA-Server message which contains an EAP Identity Request, and the result code field of this PA-Server message is set as AUTHENTICATION-REQUIRED. In addition, the server MUST assign a random session identifier to distinctly identify this session, and fill the identifier into the Session ID field of the Authentication OpCode in the PA-Server message. The Sequence Number field of the Authentication OpCode is set as 0. If there is a nonce option in the received PA-Initiation message, the PA-Server message MUST be attached with a nonce option so as to send the nonce value back. The nonce will then be used by the PCP client to check the freshness of this message. From now on, every PCP message within this session will be attached with this session identifier. When receiving a PA message from an unknown session, a PCP device MUST discard the message silently. If the PCP client intends to simplify the authentication process, it MAY append an EAP Identity Response message within the PA-Initiation message so as to inform the PCP server that it would like to perform EAP authentication and skip the step of waiting for the EAP Identity Request.

In the scenario where a PCP server receives a common PCP request message from a PCP client which needs to be authenticated, the PCP server can reply with a PA-Server message to initiate a PA session. The result code field of this PA-Server message is set as AUTHENTICATION-REQUIRED. In addition, the PCP server MUST assign a session ID for the session and transfer it within the PA-Server message. The Sequence Number field in the PA-Server is set as 0. In the PA messages exchanged afterwards in this session, the session ID MUST be used in order to help session partners distinguish the messages within this session from those not within. When the PCP client receives this initial PA-Server message from the PCP server, it can reply with a PA-Client message or silently discard the request message according to its local policies. In the PA-Client message, a nonce option which consists of a random nonce MAY be appended. If so, in the next PA-Server message, the PCP sever MUST forward the nonce back within a nonce option.

In a PA session, an EAP request message is transported within a PA-Server message, and an EAP answer message is transported within a PA-Client message. EAP relies on the underlying protocol to provide reliable transmission; any disordered delivery or loss of packets occurred during transportation must be detected and addressed. Therefore, after sending out a PA-Server message, the PCP server will not send a new PA-Server message until it receives a PA-Client message with a proper sequence number from the PCP client, and vice versa. If a PCP device receives a PA message from its partner and cannot generate a EAP response within a pre-specified period due to

certain reasons (e.g., waiting for human input to construct a EAP message or waiting for the additional PA messages in order to construct a complete EAP message), the PCP device MUST reply with a PA-Acknowledge message (PA messages with a Received Packet Option) to notify the packet has been received. This approach not only can avoid un-necessarily retransmission of the PA message but also can guarantee the reliable packet delivery in the conditions where a PCP device needs to receive multiple PA messages before generating an EAP response.

In this approach, it is mandated for a PCP client and a PCP server to perform a key-generating EAP method in authentication. Therefore, after a successful authentication procedure, a Master Session Key (MSK) will be generated. If the PCP client and the PCP server want to generate a traffic key using the MSK, they need to agree upon a Pseudo-Random Function (PRF) for the transport key derivation and a MAC algorithm to provide data origin authentication for subsequent PCP packets. In order to do this, the PCP server needs to append a set of PRF Options and MAC Algorithm Options to the initial PA-Server message. Each PRF Option contains a PRF that the PCP server supports, and each MAC Algorithm Option contains a MAC (Message Authentication Code) algorithm that the PCP server supports. Moreover, in the first PA-Server message, the server MAY also attach a ID Indication Option to direct the client to choose correct credentials. After receiving the options, the PCP client selects the PRF and the MAC algorithm which it would like to use, and then attach the associated PRF and MAC Algorithm Options to the next PA-Client message.

After the EAP authentication, the PCP server sends out a PA-Server message to indicate the EAP authentication and PCP authorization results. If the EAP authentication succeeds, the result code of the PA-Server message is AUTHENTICATION-SUCCEED. In this case, before sending out the PA-Server message, the PCP server MUST generate a PCP SA and use the derived transport key to generate a digest for the message. The digest is transported within an Authentication Tag Option for PCP Auth. A more detailed description of generating the authentication data can be found in [Section 7.1](#). In addition, the PA-Server MAY also contain a Session Lifetime Option which indicates the life-time of the PA session (i.e., the life-time of the MSK). After receiving the PA-Server message, the PCP client then needs to generate a PA-Client message as response. If the PCP client also authenticates the PCP server, the result code of the PA-Client is AUTHENTICATION-SUCCEED. In addition, the PCP client needs to generate a PCP SA and uses the derived traffic key to secure the message. From then on, all the PCP messages within the session are secured with the traffic key and the MAC algorithm specified in the PCP SA, unless a re-authentication is performed.

If a PCP client/server cannot authenticate its session partner, the device sends out a PA message with the result code, AUTHENTICATION-FAILED. If the EAP authentication succeeds but Authorization fails, the device making the decision sends out a PA message with the result code, AUTHORIZATION-FAILED. In these two cases, after the PA message is sent out, the PA session MUST be terminated immediately.

3.2. Session Termination

A PA session can be explicitly terminated by sending a termination-indicating PA message (a PA message with a result code "SESSION-TERMINATION") from either session partner. After receiving a Termination-Indicating message from the session partner, a PCP device MUST respond with a Termination-Indicating PA message and remove the PA SA immediately. When the session partner initiating the termination process receives the PA message, it will remove the associated PA SA immediately.

3.3. Session Re-Authentication

A session partner may select to perform EAP re-authentication if it would like to update the PCP SA (e.g., update the MSK and rollback the sequence numbers, or extend the session life period) without initiating a new PA session.

When the PCP server would like to initiate a re-authentication, it sends the PCP client a PA-Server message. The result code of the message is set to "RE-AUTHENTICATION", which indicates the message is for an re-authentication process. If the PCP client would like to start the re-authentication, it will send an PA-Client message to the PCP server, the result code of the PA-Client message is set to "RE-AUTHENTICATION". Then, the session partners exchange PA messages to transfer EAP messages for the re-authentication. During the re-authentication procedure, the session partners protect the integrity of PA messages with the key and MAC algorithm specified in the current PCP SA; the sequence numbers associated with the packet will never be rolled back and keep increasing according to [Section 7.3](#).

If the EAP re-authentication succeeds, the result code of the last PA-Server is "AUTHENTICATION-SUCCEED". In this case, before sending out the PA-Server, the PCP server must update the SA and use the new key to generate digests to protect the integrity and authenticity of the PA-Server and any subsequent PCP message. In addition, the PA-Server MAY be appended with a Session Lifetime Option which indicates the new life-time of the PA session.

If the EAP authentication fails, the result code of the last PA-Server is "AUTHENTICATION-FAILED". If the EAP authentication

succeeds but Authorization fails, the result code of the last PA-Server is "AUTHORIZATION-FAILED". In the latter two cases, the PA session MUST be terminated immediately after the last PA message exchange.

4. PA Security Association

At the beginning of a PA session, a session SHOULD generate a PA SA to maintain its state information during the session. The parameters of a PA SA are listed as follows:

- o IP address and UDP port number of the PCP client
- o IP address and UDP port number of the PCP server
- o Session Identifier
- o Sequence number for the next outgoing PA message
- o Sequence number for the next incoming PA message
- o Sequence number for the next outgoing common PCP message (included in the SA for PCP client)
- o Sequence number for the next incoming common PCP message (included in the SA for PCP client)
- o Last outgoing message payload
- o Retransmission interval
- o MSK: The master session key generated by the EAP method.
- o MAC algorithm: The algorithm that the transport key should use to generate digests for PCP messages.
- o Pseudo-random function: The pseudo random function negotiated in the initial PA-Server and PA-Client exchange for the transport key derivation
- o Transport key: the key derived from the MSK to provide integrity protection and data origin authentication for the messages in the PA session. The life-time of the transport key SHOULD be identical to the life-time of the session.
- o The nonce selected by the PCP client at the initiation of the session.

- o Key ID: the ID associated with Transport key.

Particularly, the transport key is computed in the following way:
Transport key = prf(MSK, "IETF PCP"| Session_ID| Nonce| key ID),
where:

- o The prf: The pseudo-random function assigned in the Pseudo-random function parameter.
- o MSK: The master session key generated by the EAP method.
- o "IETF PCP": The ASCII code representation of the non-NULL terminated string (excluding the double quotes around it).
- o Session_ID: The ID of the session which the MSK is derived from.
- o Nonce: The nonce selected by the client and transported in the Initial PA-Client packet. If the PCP client does not select one, this value is set as 0.
- o Key ID: The ID assigned for the traffic key.

5. Result Code

This message use the result code field specified in the PCP headers to transport the information for authentication and session management. Particularly, the values of following result codes are specified.

TBD INITIATION

TBD AUTHENTICATION-REQUIRED

TBD AUTHENTICATION-FAILED

TBD AUTHENTICATION-SUCCEED

TBD AUTHORIZATION-FAILED

TBD SESSION-TERMINATION

6. Packet Format

6.1. Packet Format of PCP Auth Messages

The format of PA-Server messages is identical to the response packet format specified in [Section 7.2 of \[RFC6887\]](#).

As illustrated in Figure 1, the PA-Client messages use the requester header specified in [Section 7.1](#) of [RFC6887]. The only difference is that eight reserved bits are used to transfer the result codes (e.g., "INITIATION", "AUTHENTICATION-FAILED"). Other fields in Figure 1 are described in [Section 7.1](#) of [RFC6887].

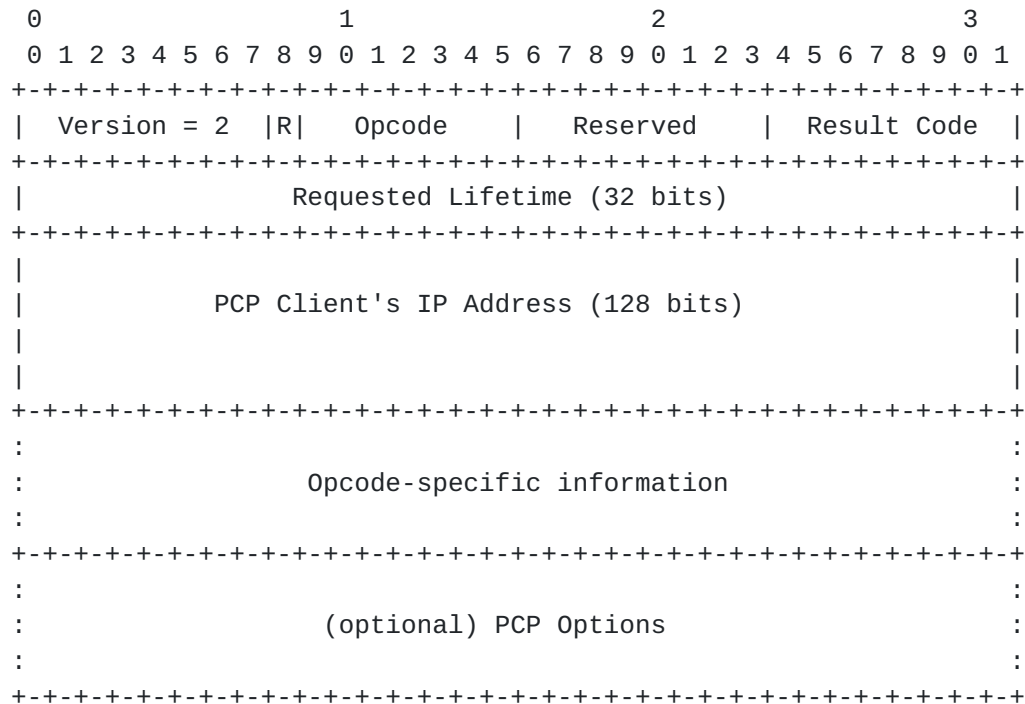
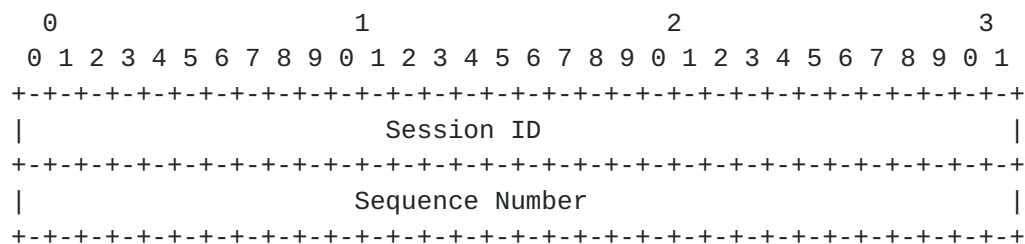


Figure 1. PA-Client message Format

6.2. Authentication OpCode

The following figure illustrates the format of an authentication OpCode:



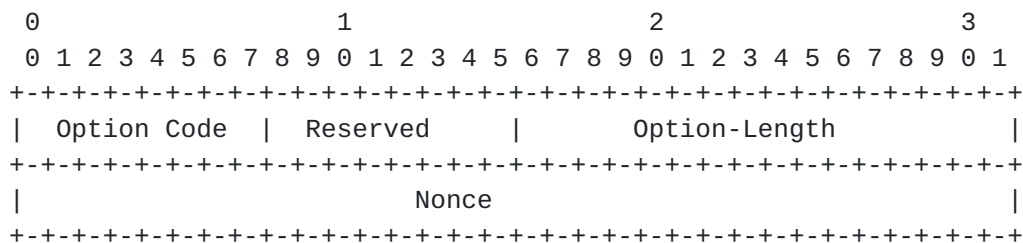
Session ID: This field contains a 32-bit PA session identifier.

Sequence Number: This field contains a 32-bit sequence number. In this solution, a sequence number needs to be incremented on every

new (non-retransmission) outgoing packet in order to provide ordering guarantee for PCP.

6.3. Nonce Option

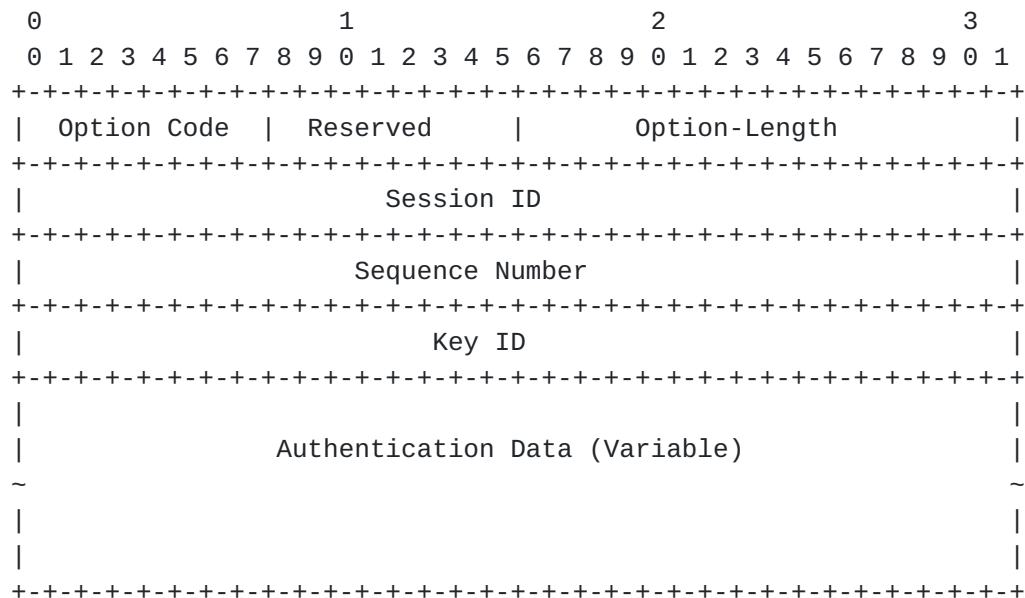
Because the session identifier of PA session is determined by the PCP server, a PCP client does not know the session identifier which will be used when it sends out a PA-Initiation message. In order to prevent an attacker from interrupting the authentication process by sending off-line generated PA-Server messages, the PCP client needs to generate a random number as nonce in the PA-Initiation message. The PCP server will append the nonce within the initial PA-Server message. If the PA-Server message does not carry the correct nonce, the message will be discarded silently.



Option-Length: The length of the Nonce Option (in octet), including the 4 octet fixed header and the variable length of the authentication data.

Nonce: A random 32 bits number which is transported within a PCC-Initiate message and the corresponding reply message from the PCP server.

6.4. Authentication Tag Option for Common PCP



Because there is no authentication OpCode in common PCP messages, the authentication tag for common PCP messages needs to provide the information of session ID and sequence numbers.

Option-Length: The length of the Authentication Tag Option for Common PCP (in octet), including the 12 octet fixed header and the variable length of the authentication data.

Session ID: A 32-bit field used to indicate the identifier of the session that the message belongs to and identifies the secret key used to create the message digest appended to the PCP message.

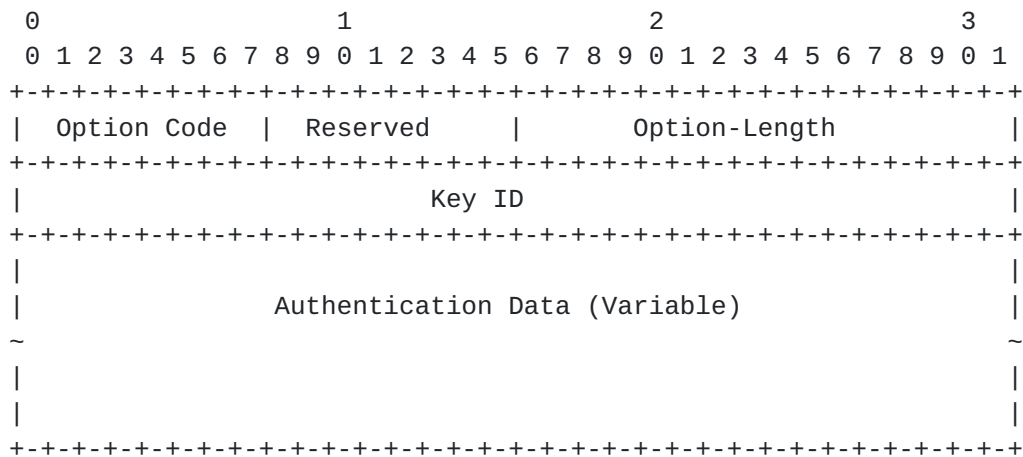
Sequence Number: This field contains a 32-bit sequence number. In this solution, a sequence number needs to be incremented on every new (non-retransmission) outgoing packet in order to provide ordering guarantee for common PCP messages.

Key ID: The ID associated with the traffic key used to generate authentication data. This field is filled with zero if MSK is directly used to secure the message.

Authentication Data: A variable-length field that carries the Message Authentication Code for the PCP packet. The generation of the digest can be various according to the algorithms specified in different PCP SAs. This field MUST end on a 32-bit boundary, padded with 0's when necessary.

6.5. Authentication Tag Option for PCP Auth Messages

This option is used to provide message authentication for PA messages. Compared with the Authentication Tag Option for Common PCP, the session ID field and the sequence number field are removed because such information is provided in the Authentication OpCode.

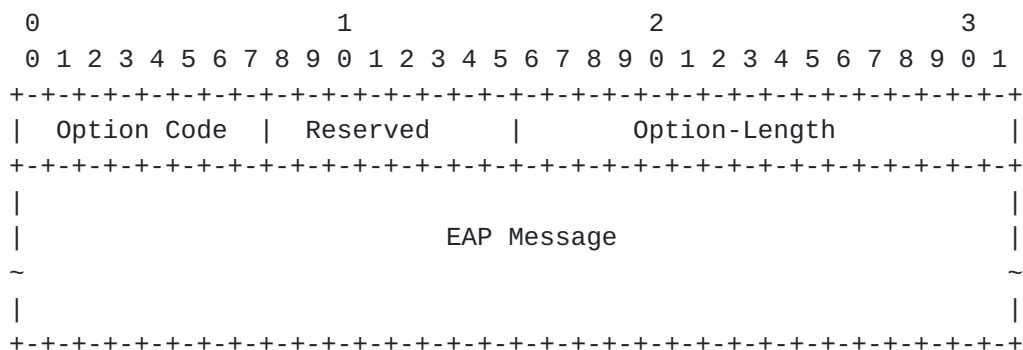


Option-Length: The length of the Authentication Tag Option for PCP Auth (in octet), including the 12 octet fixed header and the variable length of the authentication data.

Key ID: The ID associated with the traffic key used to generate authentication data. This field is filled with zero if MSK is directly used to secure the message.

Authentication Data: A variable-length field that carries the Message Authentication Code for the PCP packet. The generation of the digest can be various according to the algorithms specified in different PCP SAs. This field **MUST** end on a 32-bit boundary, padded with 0's when necessary.

6.6. EAP Payload Option



Option-Length: The length of the EAP Payload Option (in octet), including the 4 octet fixed header and the variable length of the EAP message.

EAP Message: The EAP message transferred. Note this field MUST end on a 32-bit boundary, padded with 0's when necessary.

6.7. PRF Option

```

      0               1               2               3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| Option Code | Reserved   |      Option-Length      |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                     PRF                                     |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

Option-Length: The length of the PRF Option (in octet), including the 4 octet fixed header and the variable length of the EAP message.

PRF: The Pseudo-Random Function which the sender supports to generate an MSK. This field contains an IKEv2 Transform ID of Transform Type 2 [[RFC4306](#)][RFC4868]. A PCP implementation MUST support PRF_HMAC_SHA2_256 (5).

6.8. MAC Algorithm Option

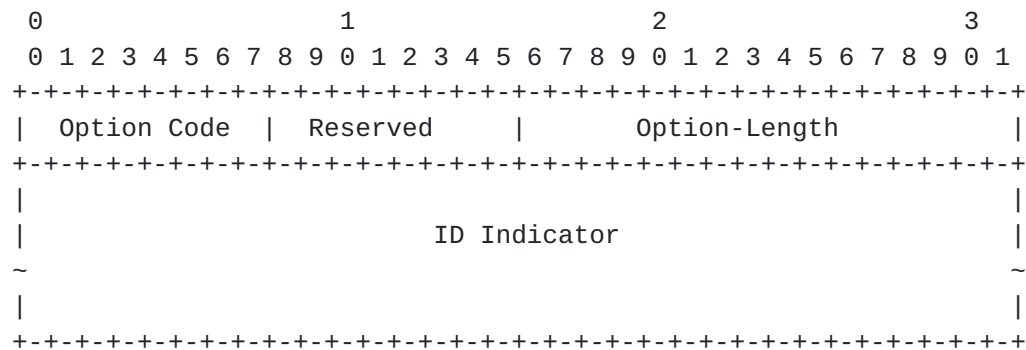
```

      0               1               2               3
    0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
| Option Code | Reserved   |      Option-Length      |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                                     MAC Algorithm ID                                     |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+

```

Option-Length: The length of the MAC Algorithm Option (in octet), including the 4 octet fixed header and the variable length of the EAP message.

MAC Algorithm ID: Indicate the MAC algorithm which the sender supports to generate authentication data. The MAC Algorithm ID field contains an IKEv2 Transform ID of Transform Type 3 [[RFC4306](#)][RFC4868]. A PCP implementation MUST support AUTH_HMAC_SHA2_256_128 (12).



Option-Length: The length of the ID Indication Option (in octet), including the 4 octet fixed header and the variable length of the EAP message.

ID Indicator: The value for a PCP client to choose proper credentials for authentication. The method of generating this value is out of scope of this document. Note this field MUST end on a 32-bit boundary, padded with 0's when necessary.

7. Processing Rules

7.1. Authentication Data Generation

If a PCP SA is generated as the result of a successful EAP authentication process, every subsequent PCP message within the session MUST carry an Authentication Tag Option which contains the digest of the PCP message for data origin authentication and integrity protection.

Before generating a digest for a PA message, a device needs to first locate the PCP SA according to the session identifier and then get the traffic key. Then the device appends an Authentication Tag Option for PCP Auth at the end of the PCP Auth message. The length of the Authentication Data field is decided by the MAC algorithm adopted in the session. The device then fills the Key ID field with the key ID of the traffic key, and sets the Authentication Data field to 0. After this, the device generates a digest for the entire PCP message (including the PCP header and Authentication Tag Option) using the traffic key and the associated MAC algorithm, and insert the generated digest into the Authentication Data field.

Similar to generating a digest for a PA message, before generating a digest for a common PCP message, a device needs to first locate the PCP SA according to the session identifier and then get the traffic key. Then the device appends the Authentication Tag Option for common PCP at the end of the message. The length of the Authentication Data field is decided by the MAC algorithm adopted in

the session. The device then use the corresponding values derived from the SA to fills the Session ID field, the Sequence Number field, and the Key ID field, and sets the Authentication Data field to 0. After this, the device generates a digest for the entire PCP message (including the PCP header and Authentication Tag Option) using the traffic key and the associated MAC algorithm, and inputs the generated digest into the Authentication Data field.

7.2. Authentication Data Validation

When a device receives a common PCP packet with an Authentication Tag Option for Common PCP, the device needs to use the session ID transported in the option to locate the proper SA, and then find the associated transport key (using key ID in the option) and the MAC algorithm. If no proper SA or traffic key is found, the PCP packet MUST be discarded silently. After storing the value of the Authentication field of the Authentication Tag Option, the device fills the Authentication field with zeros. Then, the device generates a digest for the packet (including the PCP header and Authentication Tag Option) with the transport key and the MAC algorithm found in the first step. If the value of the newly generated digest is identical to the stored one, the device can ensure that the packet has not been tampered with, and the validation succeeds. Otherwise, the packet MUST be discarded.

Similarly, when a device receives a PA message with an Authentication Tag Option for PCP Auth, the device needs to use the session ID transported in the opcode to locate the proper SA, and then find the associated transport key (using key ID in the option) and the MAC algorithm. If no proper SA or traffic key is found, the PCP packet MUST be discarded silently. After storing the value of the Authentication field of the Authentication Tag Option, the device fills the Authentication field with zeros. Then, the device generates a digest for the packet (including the PCP header and Authentication Tag Option) with the transport key and the MAC algorithm found in the first step. If the value of the newly generated digest is identical to the stored one, the device can ensure that the packet has not been tampered with, and the validation succeeds. Otherwise, the packet MUST be discarded.

7.3. Retransmission Policies for PCP Auth Messages

Because EAP relies on the underlying protocols to provide reliable transmission, after sending a PA message, a PCP client/server MUST NOT send out any subsequent messages until receiving an expect PA message (the PA message with a proper sequence number) from the peer. If no such a message is received in a certain period, the PCP device will re-send the last message according to certain retransmission

policies. This work reuses the retransmission policies specified in the base PCP protocol ([Section 8.1.1 of \[RFC6887\]](#)). In the base PCP protocol, such retransmission policies are only applied by PCP clients. However, in this work, such retransmission policies are also applied by the PCP servers.

Note that the last PA messages transported within the phases of session initiation, session re-authentication, and session termination do not have to follow the above policies since the devices sending out those messages do not expect any further PA messages.

When a device receives such a duplicate PA message from its session partner, it MUST try to answer it by sending the last outgoing PA message again. In order to achieve this function, the device needs to maintain the last incoming and the associated outgoing packet. In this case, if no outgoing PA message has been generated for the received duplicate PA message yet, the device needs to generate a PA-Acknowledgement message and sends it out. The rate of replying the duplicate PA messages MUST be limited.

7.4. Sequence Numbers for PCP Auth Messages

PCP adopts UDP to transport signaling messages. As an un-reliable transport protocol, UDP does not guarantee ordered packet delivery and does not provide any protection from packet loss. In order to ensure the EAP messages are exchanged in a reliable way, every PCP packet exchanged during EAP authentication must carry an monotonically increasing sequence number. During a PA session, a PCP device needs to maintain two sequence numbers for PA messages, one for incoming PA messages and one for outgoing PA messages. When generating an outgoing PA packet, the device attaches the associated outgoing sequence number to the packet and increments the sequence number maintained in the SA by 1. When receiving a PA packet from its session partner, the device will not accept it if the sequence number carried in the packet does not match the incoming sequence number the device maintains. After confirming that the received packet is valid, the device increments the incoming sequence number maintained in the SA by 1.

The above rules are not applied to PA-Acknowledgement messages (i.e., PA messages containing a Received Packet Option). A PA-Acknowledgement message does not transport any EAP message and only indicate at a PA message is received. Therefore, the reliable transmission of PA-Acknowledgement message does not have to be guaranteed. For instance, after sending out a PA-Acknowledgement message, a device generates a EAP response. In this case, the device should send it to its session partner directly and need not to

confirm whether the PA-Acknowledgement message has been received by its session partner or not. Therefore, when receiving or sending out a PA-Acknowledgement message, the device MUST not increase the corresponding sequence number stored in the SA. Otherwise, the lost of a PA-Acknowledgement message during transportation will cause the mismatching issues with the sequence numbers.

Another exception is in the message retransmission scenarios. When a device does not receive any response from its session partner in a certain period, it needs to retransmit the last outgoing PA message with a limited rate. The duplicate messages and the original message MUST use the identical sequence number. When the device receives such a duplicate PA message from its session partner, it MUST try to answer it by sending the last outgoing PA message again. Note the rate of replying the duplicate PA messages must be limited. In such cases, the maintained incoming and outgoing sequence numbers will not be affected by the message retransmission.

7.5. Sequence Numbers for Common PCP Messages

When transporting common PCP messages within a PA session, a PCP device needs to maintain a sequence number for outgoing common PCP messages and a sequence number for incoming common PCP messages. When generating a new outgoing PCP messages, the PCP device attaches the outgoing sequence number for common PCP messages to the messages and increments the sequence number maintained in the SA by 1.

When receiving a PCP packet from its session partner, the PCP device will not accept it if the sequence number carried in the packet is smaller than the incoming sequence number the server maintains. This approach can protect the PCP server from replay attacks. After confirming that the received packet is valid, the PCP server will use the sequence number in the incoming packet to take place the incoming sequence number for common PCP messages maintained in the SA.

Note that the sequence number in the incoming packet may not exactly match the incoming sequence number maintained locally. In the base PCP specification [[RFC6887](#)], a PCP client may stop retransmitting a PCP request without receiving any expected PCP answer when the client is no longer interested in the PCP transaction. After that, the PCP client will try to generate new PCP requests for other purposes. In this case, the sequence number in the new request will be larger than the incoming sequence number maintained in the PCP server.

7.6. MTU Considerations

EAP methods are responsible for MTU handling, so no special facilities are required in this protocol to deal with MTU issues. If an EAP message is too long for a single PA message to transport, it will be divided into multiple sections and transport them within different PA messages. Note that the receiver may not be able to know what to do in the next step until receiving all the sections and constructing the complete EAP message. In this case, in order to guarantee reliable message transmission, after receiving a PA message, the receiver **MUST** reply with a PA-Acknowledgement message until all the sections have been received.

8. IANA Considerations

TBD

9. Security Considerations

This section applies only to the in-band key management mechanism. It will need to be updated if the WG choose to pursue the out-of-band key management mechanism discussed above.

In this work, after a successful EAP authentication process performed between two PCP devices, a MSK will be exported. The MSK can be used to derive the transport keys to generate MAC digests for subsequent PCP message exchanges. However, before a transport key has been generated, the PA messages exchanged within a PA session have little cryptographic protection, and if there is no already established security channel between two session partners, these messages are subject to man-in-the-middle attacks and DOS attacks. For instance, the initial PA-Server and PA-Client exchange is vulnerable to spoofing attacks as these messages are not authenticated and integrity protected. In addition, because the PRF and MAC algorithms are transported at this stage, an attacker may try to remove the PRF and MAC options containing strong algorithms from the initial PA-Server message and force the client choose the weakest algorithms. Therefore, the server needs to guarantee that all the PRF and MAC algorithms it provides support are strong enough.

In order to prevent very basic DOS attacks, a PCP device **SHOULD** generate state information as little as possible in the initial PA-Server and PA-Client exchanges. The choice of EAP method is also very important. The selected EAP method must be resilient to the attacks possibly in an insecure network environment, and the user-identity confidentiality, protection against dictionary attacks, and session-key establishment must be supported.

10. Acknowledgements

11. Change Log

11.1. Changes from wasserman-pcp-authentication-02 to ietf-pcp-authentication-00

- o Added discussion of in-band and out-of-band key management options, leaving choice open for later WG decision.
- o Removed support for fragmenting EAP messages, as that is handled by EAP methods.

11.2. Changes from wasserman-pcp-authentication-01 to -02

- o Add a nonce into the first two exchanged PCP-Auth message between the PCP client and PCP server. When a PCP client initiate the session, it can use the nonce to detect offline attacks.
- o Add the key ID field into the authentication tag option so that a MSK can generate multiple traffic keys.
- o Specify that when a PCP device receives a PCP-Auth-Server or a PCP-Auth-Client message from its partner the PCP device needs to reply with a PCP-Auth-Acknowledge message to indicate that the message has been received.
- o Add the support of fragmenting EAP messages.

11.3. Changes from ietf-pcp-authentication-00 to -01

- o Editorial changes, added use cases to introduction.

11.4. Changes from ietf-pcp-authentication-01 to -02

- o Add the support of re-authentication initiated by PCP server.
- o Specify that when a PCP device receives a PCP-Auth-Server or a PCP-Auth-Client message from its partner the PCP device MAY reply with a PCP-Auth-Acknowledge message to indicate that the message has been received.
- o Discuss the format of the PCP-Auth-Acknowledge message.
- o Remove the redundant information from the Auth OpCode, and specify new result codes transported in PCP packet headers
- o

11.5. Changes from ietf-pcp-authentication-02 to -03

- o Change the name "PCP-Auth-Request" to "PCP-Auth-Server"
- o Change the name "PCP-Auth-Response" to "PCP-Auth-Client"
- o Specify two new sequence numbers for common PCP messages in the PCP SA, and describe how to use them
- o Specify a Authentication Tag Option for PCP Common Messages
- o Introduce the scenario where a EAP message has to be divided into multiple sections and transported in different PCP-Auth messages (for the reasons of MTU), and introduce how to use PCP-Auth-Acknowledge messages to ensure reliable packet delivery in this case.

11.6. Changes from ietf-pcp-authentication-03 to -04

- o Change the name "PCP-Auth" to "PA".
- o Refine the retransmission policies.
- o Provide the discussion about how to instruct a PCP client to choose proper credential during authentication, and an ID Indication Option is defined for that purpose.

12. References

12.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.

12.2. Informative References

- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.
- [RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", [RFC 4306](#), December 2005.
- [RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", [RFC 4868](#), May 2007.

- [RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", [RFC 5191](#), May 2008.
- [RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", [RFC 5448](#), May 2009.
- [RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", [RFC 6887](#), April 2013.

Authors' Addresses

Margaret Wasserman
Painless Security
356 Abbott Street
North Andover, MA 01845
USA

Phone: +1 781 405 7464
Email: mrw@painless-security.com
URI: <http://www.painless-security.com>

Sam Hartman
Painless Security
356 Abbott Street
North Andover, MA 01845
USA

Email: hartmans@painless-security.com
URI: <http://www.painless-security.com>

Dacheng Zhang
Huawei
Beijing
China

Email: zhangdacheng@huawei.com

