

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 31, 2015

M. Wasserman
S. Hartman
Painless Security
D. Zhang
Huawei
T. Reddy
Cisco
June 29, 2015

Port Control Protocol (PCP) Authentication Mechanism
draft-ietf-pcp-authentication-12

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 communication 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 describes 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 December 31, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](http://trustee.ietf.org/license-info) 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
3.1.1.	Authentication triggered by the client	6
3.1.2.	Authentication triggered by the server	7
3.1.3.	Authentication using EAP	8
3.2.	Session Termination	9
3.3.	Session Re-Authentication	9
4.	PA Security Association	10
5.	Packet Format	12
5.1.	Packet Format of PCP Auth Messages	12
5.2.	Opcode-specific information of AUTHENTICATION Opcode	13
5.3.	NONCE Option	13
5.4.	AUTHENTICATION_TAG Option	14
5.5.	PA_AUTHENTICATION_TAG	15
5.6.	EAP_PAYLOAD Option	16
5.7.	PRF Option	16
5.8.	MAC_ALGORITHM Option	17
5.9.	SESSION_LIFETIME Option	17
5.10.	RECEIVED_PAK Option	17
5.11.	ID_INDICATOR Option	18
6.	Processing Rules	19
6.1.	Authentication Data Generation	19
6.2.	Authentication Data Validation	20
6.3.	Retransmission Policies for PA Messages	20
6.4.	Sequence Numbers for PCP Auth Messages	21
6.5.	Sequence Numbers for Common PCP Messages	22
6.6.	MTU Considerations	23
7.	IANA Considerations	23
7.1.	NONCE	24

7.2.	AUTHENTICATION_TAG	24
7.3.	PA_AUTHENTICATION_TAG	25
7.4.	EAP_PAYLOAD	25
7.5.	PRF	25
7.6.	MAC_ALGORITHM	26
7.7.	SESSION_LIFETIME	26
7.8.	RECEIVED_PAK	26
7.9.	ID_INDICATOR	27
8.	Security Considerations	27
9.	Acknowledgements	28
10.	Change Log	28
10.1.	Changes from wasserman-pcp-authentication-02 to ietf-pcp-authentication-00	28
10.2.	Changes from wasserman-pcp-authentication-01 to -02	28
10.3.	Changes from ietf-pcp-authentication-00 to -01	29
10.4.	Changes from ietf-pcp-authentication-01 to -02	29
10.5.	Changes from ietf-pcp-authentication-02 to -03	29
10.6.	Changes from ietf-pcp-authentication-03 to -04	29
10.7.	Changes from ietf-pcp-authentication-04 to -05	30
10.8.	Changes from ietf-pcp-authentication-05 to -06	30
11.	References	30
11.1.	Normative References	30
11.2.	Informative References	31
	Authors' Addresses	31

[1.](#) Introduction

Using the Port Control Protocol (PCP) [[RFC6887](#)], an application 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 defines a PCP security extension that enables PCP servers to authenticate their clients with Extensible Authentication Protocol (EAP). The EAP messages are encapsulated within PCP messages during transportation.

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

- o Loss of EAP messages during transportation
- o Reordered 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 do not create implicit mappings for specific traffic.
- 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 applications to create mappings for successful inbound communications destined to machines located behind a NAT or a firewall.

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 software instance that 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 software instance that resides on the PCP-Controlled Device that receives PCP requests from the PCP client and creates appropriate state in response to that request. 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 messages involved within a session includes the PCP Authentication (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 implementation involved within a PA session. Each PA session has two session partners (a PCP server and a PCP client).

PCP device: A PCP client or a PCP server.

Session Lifetime: The lifetime 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 message, while a PA message sent from a PCP client to a PCP server is referred to as a PA-Client message. Therefore, a PA-Server message is actually a PCP response message specified in [\[RFC6887\]](#), and a PA-Client message is a PCP request message. This document specifies an option, the PA_AUTHENTICATION_TAG Option defined in [Section 5.5](#) for PCP authentication, 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 AUTHENTICATION_TAG Option 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 MUST contain an AUTHENTICATION Opcode and may optionally contain a set of Options for various purposes (e.g., transporting authentication messages and

session management). The opcode-specific information in a AUTHENTICATION Opcode consists of two fields : Session ID and Sequence Number. The Session ID field is used to identify the PA session to which the message belongs. The sequence number field is used to detect whether reordering or duplication occurred during message delivery.

3.1.1. Authentication triggered by the client

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. [Section 5.1](#) updates the PCP request message format to have a result code. In the message, the Session ID and Sequence Number fields of the AUTHENTICATION Opcode are set as 0. The PA-Client message SHOULD also contain a NONCE option defined in [Section 5.3](#) which consists of a random nonce.

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 to 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 contain 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 PA session MUST contain 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.


```

PCP client                                PCP server
| -- PA-Initiation----->|
|   (Seq=0, Session ID=0)      |
|                               |
|<-- PA-Server -----|
|   (Seq=0, Session ID=X, EAP Identity request) |
|                               |
| -- PA-Client ----->|
|   (Seq=1, Session ID=X, EAP Identity response) |
|                               |
|<-- PA-Server -----|
|   (Seq=1, Session ID=X, EAP Identity request) |

```

3.1.2. Authentication triggered by the server

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 to 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 message is set as 0. In the PA messages exchanged afterwards in this session, the Session ID will 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 server MUST forward the nonce back within a NONCE option.

```

PCP client                                PCP server
| -- Common PCP request----->|
|                               |
|<-- PA-Server -----|
|   (Seq=0, Session ID=X, EAP Identity request) |
|                               |
| -- PA-Client ----->|
|   (Seq=0, Session ID=X, EAP Identity response) |
|                               |
|<-- PA-Server -----|
|   (Seq=1, Session ID=X, EAP Identity request) |

```


3.1.3. Authentication using EAP

In a PA session, an EAP Identity request message is transported within a PA-Server message, and an EAP Identity response message is transported within a PA-Client message. EAP relies on the underlying protocol to provide reliable transmission; any reordered delivery or loss of packets occurring 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 client receives a PA message containing an EAP Identity request and cannot generate an EAP Identity response immediately 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-Acknowledgement message (PA message with a RECEIVED_PAK Option) to indicate that the message has been received. This approach not only can avoid unnecessary retransmission of the PA message but also can guarantee the reliable message delivery in the conditions where a PCP device needs to receive multiple PA messages before generating an EAP Identity response.

In this approach, PCP client and a PCP server **MUST** perform a key-generating EAP method in authentication. Particularly, a PCP authentication implementation **MUST** support EAP-TTLS [[RFC5281](#)] and **SHOULD** support TEAP [[RFC7170](#)]. 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 transport 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 messages. 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 an ID_INDICATOR Option defined in [Section 5.11](#) to direct the client to choose correct credentials. After receiving the options, the PCP client **MUST** select the PRF and the MAC algorithm which it would like to use, and then adds 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_SUCCEEDED. 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 PA_AUTHENTICATION_TAG Option for PCP Auth. A more detailed description of generating the authentication data can be found in [Section 6.1](#). In addition, the PA-Server message MAY also contain a SESSION_LIFETIME Option defined in [Section 5.9](#) which indicates the lifetime of the PA session (i.e., the lifetime 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 message is AUTHENTICATION_SUCCEEDED. In addition, the PCP client needs to generate a PCP SA and uses the derived transport key to secure the message. From then on, all the PCP messages within the session are secured with the transport key and the MAC algorithm specified in the PCP SA, unless a re-authentication is performed. The first secure PA-client message from the client MUST include the set of PRF and MAC_ALGORITHM options received from the PCP server. The PCP server determines if the set of algorithms conveyed by the client matches the set it had initially sent, to detect an algorithm downgrade attack. If the server detects a downgrade attack then it MUST send a PA-Server message with result code DOWNGRADE_ATTACK_DETECTED and terminate the session.

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_TERMINATED") 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 without initiating a new PA session. For example a re-authentication procedure could be triggered for the following reasons:

- o The session lifetime needs to be extended.
- o The sequence number is going to reach the maximum value.
Specifically, when the sequence number reaches $2^{32} - 2^{16}$, the session partner MUST trigger re-authentication.

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 a re-authentication process. If the PCP client would like to start the re-authentication, it will send a PA-Client message to the PCP server, with the result code of the PA-Client message 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 message will continue to keep increasing according to [Section 6.3](#).

If the EAP re-authentication succeeds, the result code of the last PA-Server message is "AUTHENTICATION_SUCCEEDED". In this case, before sending out the PA-Server message, the PCP server MUST update the SA and use the new key to generate a digest for the PA-Server message and subsequent PCP messages. In addition, the PA-Server message MAY be appended with a SESSION_LIFETIME Option which indicates the new lifetime of the PA session. PA and PCP message sequence numbers must also be reset to zero.

If the EAP authentication fails, the result code of the last PA-Server message is "AUTHENTICATION_FAILED". If the EAP authentication succeeds but authorization fails, the result code of the last PA-Server message is "AUTHORIZATION_FAILED". In the latter two cases, the PA session MUST be terminated immediately after the last PA message exchange.

During re-authentication, the session partners can also exchange common PCP messages in parallel. The common PCP messages MUST be protected with the current SA until the new SA has been generated.

4. PA Security Association

At the beginning of a PA session, a session MUST 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
- o Sequence number for the next incoming common PCP message
- o Last outgoing message payload
- o Retransmission interval
- o The master session key (MSK) generated by the EAP method.
- o The MAC algorithm that the transport key should use to generate digests for PCP messages.
- o The pseudo random function negotiated in the initial PA-Server and PA-Client message exchange for the transport key derivation
- o The transport key derived from the MSK to provide integrity protection and data origin authentication for the messages in the PA session. The lifetime of the transport key SHOULD be identical to the lifetime of the session.
- o The nonce selected by the PCP client at the initiation of the session.
- o The Key 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 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 '||' : is the concatenation operator.
- 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 message. If the PCP client does not select one, this value is set as 0.
- o Key ID: The ID assigned for the transport key.

5. Packet Format

5.1. Packet Format of PCP Auth Messages

The format of the PA-Server message is identical to the response message format specified in [Section 7.2 of \[RFC6887\]](#). The result code for PA-Sever message carrying EAP Identity request MUST be set to AUTHENTICATION_REQUIRED.

As illustrated in Figure 1, the PA-Client messages use the request 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 \[RFC6887\]](#).

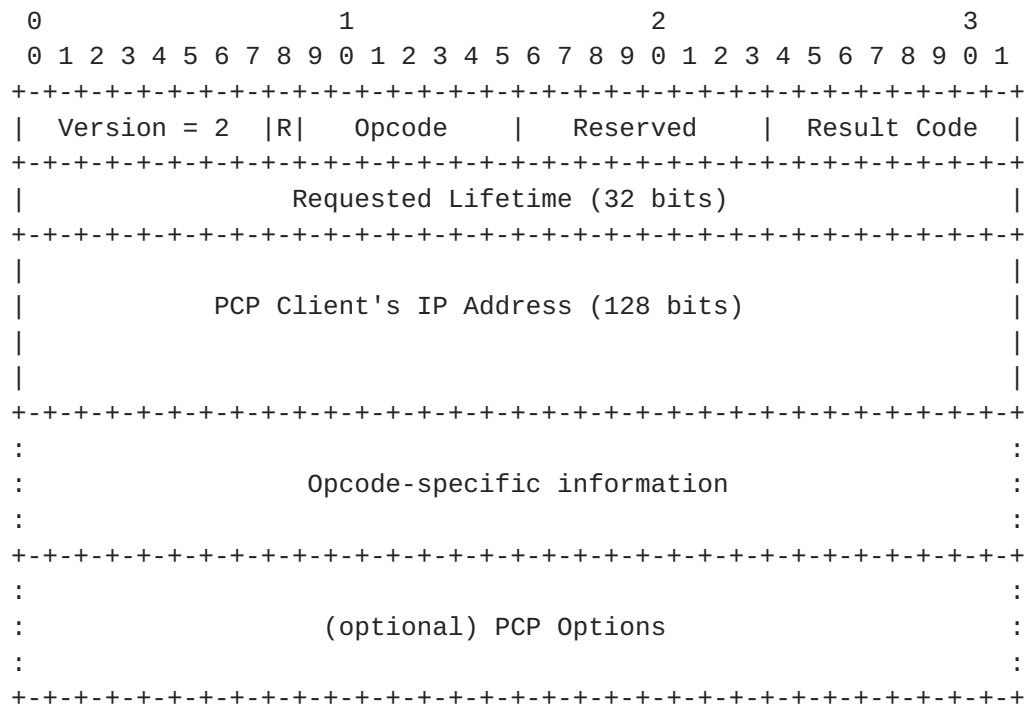


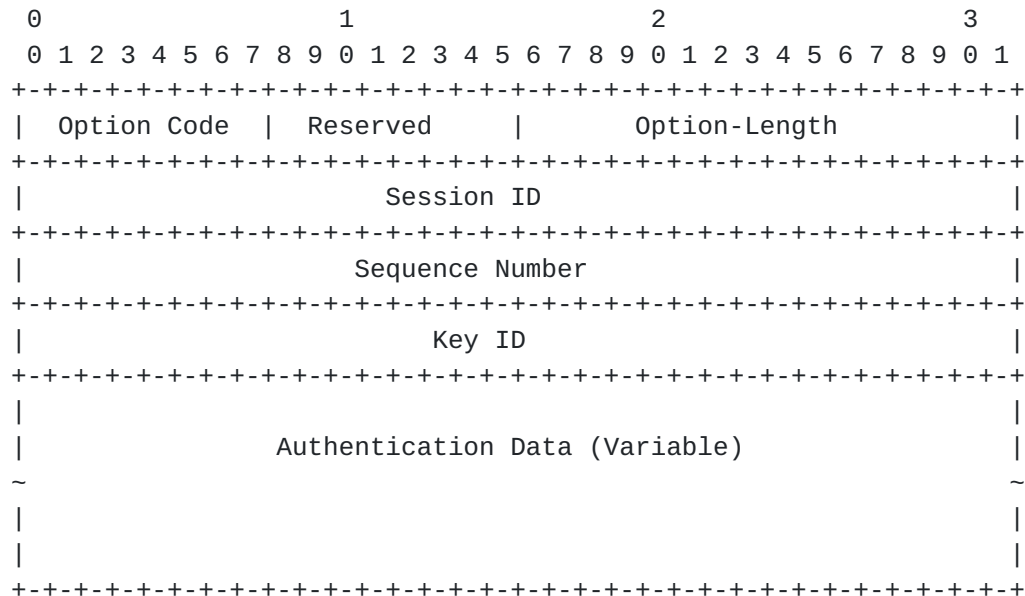
Figure 1. PA-Client message Format

The Requested Lifetime field of PA-Client message and Lifetime field of PA-Server message are both set to 0 on transmission and ignored on reception.

Option-Length: 4 octets.

Nonce: A random 32 bit number which is transported within a PA-Initiation message and the corresponding reply message from the PCP server.

5.4. AUTHENTICATION_TAG Option



Because there is no authentication Opcode in common PCP messages, the authentication tag for common PCP messages needs to carry the Session ID and Sequence Number.

Option Code: TBA-131.

Reserved: 8 bits. MUST be set to 0 on transmission and MUST be ignored on reception.

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

Session ID: A 32-bit field used to identify the session to which the message belongs and identify the secret key used to create the message digest appended to the PCP message.

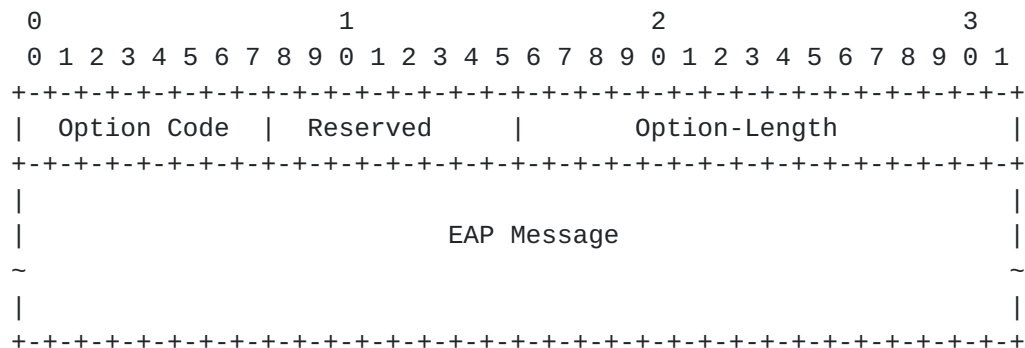
Sequence Number: A 32-bit sequence number. In this solution, a sequence number needs to be incremented on every new (non-retransmission) outgoing message in order to provide ordering guarantee for common PCP messages.

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

Authentication Data: A variable-length field that carries the Message Authentication Code for the PCP Auth message. The generation of the digest varies according to the algorithms

specified in different PCP SAs. This field **MUST** end on a 32-bit boundary, padded with null characters when necessary.

5.6. EAP_PAYLOAD Option



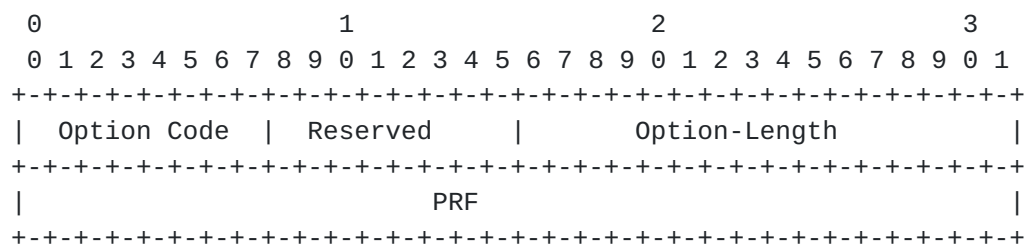
Option Code: TBA-133.

Reserved: 8 bits. MUST be set to 0 on transmission and MUST be ignored on reception.

Option-Length: Variable

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

5.7. PRF Option

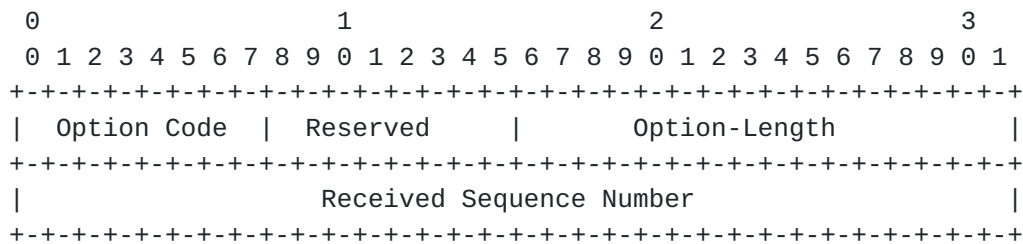


Option Code: TBA-134.

Reserved: 8 bits. MUST be set to 0 on transmission and MUST be ignored on reception.

Option-Length: 4 octets.

PRF: The Pseudo-Random Function which the sender supports to generate an MSK. This field contains an IKEv2 Transform ID of Transform Type 2 [RFC7296][RFC4868]. A PCP implementation MUST support PRF_HMAC_SHA2_256 (5).



Option Code: TBA-137.

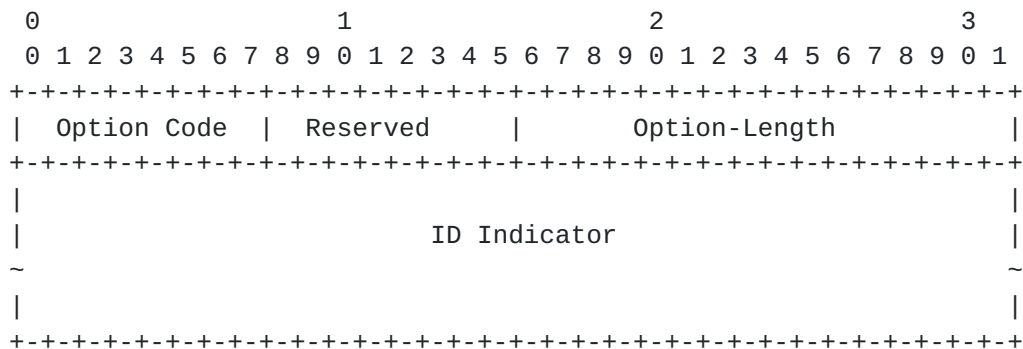
Reserved: 8 bits. MUST be set to 0 on transmission and MUST be ignored on reception.

Option-Length: 4 octets.

Received Sequence Number: The sequence number of the last received PCP message.

5.11. ID_INDICATOR Option

The ID_INDICATOR option is used by the PCP client to determine which credentials to provide to the PCP server.



Option Code: TBA-138.

Reserved: 8 bits. MUST be set to 0 on transmission and MUST be ignored on reception.

Option-Length: Variable.

ID Indicator: The identity of the authority that issued the credentials. The field MUST end on a 32-bit boundary, padded with 0's when necessary. The ID indicator field is UTF-8 encoded [RFC3629] Unicode string conforming to the "UsernameCaseMapped" profile of the PRECIS IdentifierClass [I-D.ietf-precis-saslprepbis]. The PCP client validates that the ID indicator field conforms to the "UsernameCaseMapped" profile of

the PRECIS IdentifierClass. The PCP client enforces the rules specified in section 3.2.2 of [[I-D.ietf-precis-saslprepbis](#)] to map the ID indicator field. The PCP client compares the resulting string with the ID indicators stored locally on the PCP client to pick the credentials for authentication. The two indicator strings are to be considered equivalent by the client if and only if they are an exact octet-for-octet match.

6. Processing Rules

6.1. 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 which contains the digest of the PCP message for data origin authentication and integrity protection.

- o 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 transport key. Then the device appends an PA_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 transport 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 PA_AUTHENTICATION_TAG Option) using the transport key and the associated MAC algorithm, and inserts the generated digest into the Authentication Data field.
- o 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 transport key. Then the device appends the AUTHENTICATION_TAG Option at the end of common PCP message. The length of the Authentication Data field is decided by the MAC algorithm adopted in the session. The device then uses the corresponding values derived from the SA to fill 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 transport key and the associated MAC algorithm, and inputs the generated digest into the Authentication Data field.

6.2. Authentication Data Validation

When a device receives a common PCP message with an AUTHENTICATION_TAG Option for Common PCP Messages, 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 the key ID in the option) and the MAC algorithm. If no proper SA or transport key is found or the sequence number is invalid (see [Section 6.5](#)), the PCP message 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 message (including the PCP header and Authentication Tag Option) with the transport key and the MAC algorithm. If the value of the newly generated digest is identical to the stored one, the device can ensure that the message has not been tampered with, and the validation succeeds. Otherwise, the message MUST be discarded.

Similarly, when a device receives a PA message with an PA_AUTHENTICATION_TAG Option for PCP Authentication, 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 the key ID in the option) and the MAC algorithm. If no proper SA or transport key is found or the sequence number is invalid (see [Section 6.4](#)), the PCP message MUST be discarded silently. After storing the value of the Authentication field of the PA_AUTHENTICATION_TAG Option, the device fills the Authentication field with zeros. Then, the device generates a digest for the message (including the PCP header and PA_AUTHENTICATION_TAG Option) with the transport key and the MAC algorithm. If the value of the newly generated digest is identical to the stored one, the device can ensure that the message has not been tampered with, and the validation succeeds. Otherwise, the message MUST be discarded.

6.3. Retransmission Policies for PA 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 a PA message with a proper sequence number from the peer. If no such a message is received the PCP device will re-send the last message according to 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. If Maximum retransmission duration seconds have elapsed and no expected

response is received, the device will terminate the session and discard the current SA.

As illustrated in [Section 3.1.3](#), in order to avoid unnecessary re-transmission, the device receiving a PA message MUST send a PA-Acknowledgement message to the sender of the PA message when it cannot send a PA response immediately. The PA-Acknowledgement message is used to indicate the receipt of the PA message. When the sender receives the PA-Acknowledgement message, it will stop the retransmission.

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 a re-transmitted last incoming PA message from its session partner, it MUST try to answer it by sending the last outgoing PA message again. However, if the duplicate message has the same sequence number but is not bit-wise identical to the original message then the device MUST discard it. In order to achieve this function, the device may need to maintain the last incoming and the associated outgoing messages. In this case, if no outgoing PA message has been generated for the received duplicate PA message yet, the device needs to send a PA-Acknowledgement message. The rate of replying to duplicate PA messages MUST be limited to provide robustness against denial of service (DoS) attacks. The details of rate limiting are outside the scope of this specification.

6.4. Sequence Numbers for PCP Auth Messages

PCP uses 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 message exchanged during EAP authentication must carry a 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 message, the device adds the associated outgoing sequence number to the message and increments the sequence number maintained in the SA by 1. When receiving a PA message from its session partner, the device will not accept it if the sequence number carried in the message does not match the incoming sequence number the device maintains. After confirming that the received message is valid, the device increments the incoming sequence number maintained in the SA by 1.

The above rules are not applicable to PA-Acknowledgement messages (i.e., PA messages containing a RECEIVED_PAK Option). A PA-Acknowledgement message does not transport any EAP message and only indicates that a PA message is received. Therefore, reliable transmission of PA-Acknowledgement messages is not required. For instance, after sending out a PA-Acknowledgement message, a device generates an EAP Identity response. In this case, the device need not have 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, loss of a PA-Acknowledgement message will cause a mismatch in sequence numbers.

Another exception is the message retransmission scenario. As discussed in [Section 6.3](#), when a PCP device does not receive any response from its session partner it needs to retransmit the last outgoing PA message following the retransmission procedure specified in [section 8.1.1 of \[RFC6887\]](#). The original message and duplicate messages **MUST** be bit-wise identical. When the device receives such a duplicate PA message from its session partner, it **MUST** send the last outgoing PA message again. In such cases, the maintained incoming and outgoing sequence numbers will not be affected by the message retransmission.

6.5. 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 message, the PCP device updates the Sequence Number field in the AUTHENTICATION_TAG option with the outgoing sequence number maintained in the SA and increments the outgoing sequence number by 1.

When receiving a PCP message from its session partner, the PCP device will not accept it if the sequence number carried in the message is smaller than the incoming sequence number the device maintains. This approach can protect the PCP device from replay attacks. After confirming that the received message is valid, the PCP device will update the incoming sequence number maintained in the PCP SA with the sequence number of the incoming message.

Note that the sequence number in the incoming message may not exactly match the incoming sequence number maintained locally. As discussed in the base PCP specification [\[RFC6887\]](#), if a PCP client is no longer interested in the PCP transaction and has not yet received a PCP response from the server then it will stop retransmitting the PCP

request. After that, the PCP client might generate new PCP requests for other purposes using the current SA. In this case, the sequence number in the new request will be larger than the sequence number in the old request and so will be larger than the incoming sequence number maintained in the PCP server.

Note that in the base PCP specification [RFC6887], a PCP client needs to select a nonce in each MAP or PEER request, and the nonce is sent back in the response. However, it is possible for a client to use the same nonce in multiple MAP or PEER requests, and this may cause a potential risk of replay attacks. This attack is addressed by using the sequence number in the PCP response.

6.6. MTU Considerations

EAP methods are responsible for MTU handling, so no special facilities are required in PCP to deal with MTU issues. Particularly, EAP lower layers indicate to EAP methods and AAA servers the MTU of the lower layer. EAP methods such as EAP-TLS [RFC5216], TEAP [RFC7170], and others that are likely to exceed reasonable MTUs provide support for fragmentation and reassembly. Others, such as EAP-GPSK [RFC5433] assume they will never send packets larger than the MTU and use small EAP packets.

If an EAP message is too long to be transported within a single PA message, it will be divided into multiple sections and sent within different PA messages. Note that the receiver may not be able to know what to do in the next step until it has received all the sections and reconstructed the complete EAP message. In this case, in order to guarantee reliable message transmission, after receiving a PA message, the receiver replies with a PA-Acknowledgement message to notify the sender to send the next PA message.

7. IANA Considerations

The following PCP Opcode is to be allocated in the mandatory-to-process range from the standards action range (the registry for PCP Opcodes is maintained in <http://www.iana.org/assignments/pcp-parameters>):

TBA AUTHENTICATION Opcode.

The following PCP result codes are to be allocated in the mandatory-to-process range from the standards action range (the registry for PCP result codes is maintained in <http://www.iana.org/assignments/pcp-parameters>):

TBA INITIATION: The client indication to the server for authentication.

TBA AUTHENTICATION_REQUIRED: The server indication to the client that authentication is required.

TBA AUTHENTICATION_FAILED: This error response is signaled to the client if EAP authentication had failed.

TBA AUTHENTICATION_SUCCEEDED: This success response is signaled to the client if EAP authentication had succeeded.

TBA AUTHORIZATION_FAILED: This error response is signaled to the client if the EAP authentication had succeeded but authorization failed.

TBA SESSION_TERMINATED: This PCP result code indicates to the partner that the PA session must be terminated.

TBA DOWNGRADE_ATTACK_DETECTED: This error response is signaled to the client if the server detects downgrade attack.

The following PCP Option Codes are to be allocated in the mandatory-to-process range from the standards action range (the registry for PCP Options is maintained in <http://www.iana.org/assignments/pcp-parameters>):

7.1. NONCE

Option Name: NONCE

option-code: TBA-130 in the mandatory-to-process range (IANA).

Purpose: See [Section 5.3](#).

Valid for Opcodes: Authentication Opcode.

option-len: Option Length is 4 octets.

May appear in: request and response.

Maximum occurrences: 1.

7.2. AUTHENTICATION_TAG

Option Name: AUTHENTICATION_TAG

option-code: TBA-131 in the mandatory-to-process range (IANA).

Purpose: See [Section 5.4](#).

Valid for Opcodes: MAP, PEER and ANNOUNCE Opcodes.

option-len: Variable length.

May appear in: request and response.

Maximum occurrences: 1.

[7.3.](#) PA_AUTHENTICATION_TAG

Option Name: PA_AUTHENTICATION_TAG

option-code: TBA-132 in the mandatory-to-process range (IANA).

Purpose: See [Section 5.5](#).

Valid for Opcodes: Authentication Opcode.

option-len: Variable length.

May appear in: request and response.

Maximum occurrences: 1.

[7.4.](#) EAP_PAYLOAD

Option Name: EAP_PAYLOAD.

option-code: TBA-133 in the mandatory-to-process range (IANA).

Purpose: See [Section 5.6](#).

Valid for Opcodes: Authentication Opcode.

option-len: Variable length.

May appear in: request and response.

Maximum occurrences: 1.

[7.5.](#) PRF

Option Name: PRF.

option-code: TBA-134 in the mandatory-to-process range (IANA).

Purpose: See [Section 5.7](#).

Valid for Opcodes: Authentication Opcode.

option-len: Option Length is 4 octets.

May appear in: request and response.

Maximum occurrences: as many as fit within maximum PCP message size.

[7.6.](#) MAC_ALGORITHM

Option Name: MAC_ALGORITHM.

option-code: TBA-135 in the mandatory-to-process range (IANA).

Purpose: See [Section 5.8](#).

Valid for Opcodes: Authentication Opcode.

option-len: Option Length is 4 octets.

May appear in: request and response.

Maximum occurrences: as many as fit within maximum PCP message size.

[7.7.](#) SESSION_LIFETIME

Option Name: SESSION_LIFETIME.

option-code: TBA-136 in the mandatory-to-process range (IANA).

Purpose: See [Section 5.9](#).

Valid for Opcodes: Authentication Opcode.

option-len: Option Length is 4 octets.

May appear in: response.

Maximum occurrences: 1.

[7.8.](#) RECEIVED_PAK

Option Name: RECEIVED_PAK.

option-code: TBA-137 in the mandatory-to-process range (IANA).

Purpose: See [Section 5.10](#).

Valid for Opcodes: Authentication Opcode.

option-len: Option Length is 4 octets.

May appear in: request and response.

Maximum occurrences: 1.

[7.9.](#) ID_INDICATOR

Option Name: ID_INDICATOR.

option-code: TBA-138 in the mandatory-to-process range (IANA).

Purpose: See [Section 5.11](#).

Valid for Opcodes: Authentication Opcode.

option-len: Variable length.

May appear in: response.

Maximum occurrences: 1.

[8.](#) Security Considerations

In this work, after a successful EAP authentication process is performed between two PCP devices, an MSK will be exported. The MSK will 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 message 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 for 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 message exchanges. The choice of EAP method is

also very important. The selected EAP method must be resilient to the attacks possible in an insecure network environment, provide user-identity confidentiality, protection against dictionary attacks, and support session-key establishment.

When a PCP proxy is located between a PCP server and PCP clients, the proxy may perform authentication with the PCP server before it processes requests from the clients. In addition, re-authentication between the PCP proxy and PCP server will not interrupt the service that the proxy provides to the clients since the proxy is still allowed to send common PCP messages to the PCP server during that period.

9. Acknowledgements

Thanks to Dan Wing, Prashanth Patil, Dave Thaler, Peter Saint-Andre, Carlos Pignataro, Brian Haberman and Paul Kyzivat for the valuable comments.

10. Change Log

[Note: This section should be removed by the RFC Editor upon publication]

10.1. 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.

10.2. 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 transport 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.

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

- o Editorial changes, added use cases to introduction.

10.4. 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

10.5. 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.

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

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

10.7. Changes from ietf-pcp-authentication-04 to -05

- o Add contents in IANA considerations.
- o Add discussions in fragmentation.
- o Refine the PA messages retransmission policies.
- o Add IANA considerations.

10.8. Changes from ietf-pcp-authentication-05 to -06

- o Added mechanism to handle algorithm downgrade attack.
- o Updated Security Considerations section.
- o Updated ID Indicator Option.

11. References

11.1. Normative References

- [I-D.ietf-precis-saslprepbis]
Saint-Andre, P. and A. Melnikov, "Preparation, Enforcement, and Comparison of Internationalized Strings Representing Usernames and Passwords", [draft-ietf-precis-saslprepbis-18](#) (work in progress), May 2015.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, [RFC 3629](#), November 2003.
- [RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.
- [RFC4868] Kelly, S. and S. Frankel, "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", [RFC 4868](#), May 2007.
- [RFC5281] Funk, P. and S. Blake-Wilson, "Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)", [RFC 5281](#), August 2008.
- [RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", [RFC 6887](#), April 2013.

- [RFC7170] Zhou, H., Cam-Winget, N., Salowey, J., and S. Hanna, "Tunnel Extensible Authentication Protocol (TEAP) Version 1", [RFC 7170](#), May 2014.
- [RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, [RFC 7296](#), October 2014.

11.2. Informative References

- [RFC5216] Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", [RFC 5216](#), March 2008.
- [RFC5433] Clancy, T. and H. Tschofenig, "Extensible Authentication Protocol - Generalized Pre-Shared Key (EAP-GPSK) Method", [RFC 5433](#), February 2009.
- [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.

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: zhang_dacheng@hotmail.com

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tiredddy@cisco.com

