

**Pre-authentication Support for PANA
draft-ietf-pana-preauth-03**

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on April 27, 2009.

Abstract

This document defines an extension to the Protocol for carrying Authentication for Network Access (PANA) for proactively establishing a PANA SA (Security Association) between a PaC in one access network and a PAA in another access network to which the PaC may move. The proposed method operates across multiple administrative domains.

Table of Contents

1.	Introduction	3
1.1.	Specification of Requirements	3
2.	Terminogy	3
3.	Pre-authentication Procedure	4
4.	PANA Extensions	7
5.	Authorization and Accounting Considerations	8
6.	Security Considerations	8
7.	IANA Considerations	9
8.	Acknowledgments	9
9.	References	9
9.1.	Normative References	9
9.2.	Informative References	9
	Author's Address	9
	Intellectual Property and Copyright Statements	10

1. Introduction

The Protocol for carrying Authentication for Network Access (PANA) [[RFC5191](#)] carries EAP messages between a PaC (PANA Client) and a PAA (PANA Authentication Agent) in the access network. If the PaC is a mobile device and is capable of moving one access network to another while running its applications, it is critical for the PaC to perform a handover seamlessly without degrading the performance of the applications during the handover period. When the handover requires the PaC to establish a PANA session with the PAA in the new access network, the signaling to establish the PANA session should be completed as fast as possible.

This document defines an extension to the PANA protocol [[RFC5191](#)] used for proactively executing EAP authentication and establishing a PANA SA (Security Association) between a PaC in an access network and a PAA in another access network to which the PaC may move. The proposed method operates across multiple AAA domains. The extension to the PANA protocol is designed to realize direct pre-authentication defined in [[I-D.ietf-hokey-preauth-ps](#)].

1.1. Specification of Requirements

In this document, several words are used to signify the requirements of the specification. These words are often capitalized. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

2. Terminogy

The following terms are used in this document in addition to the terms defined in [[RFC5191](#)].

Serving PAA (SPAA): A PAA that resides in the serving network and provides network access authentication for a particular PaC. For simplicity, this document assumes that there is only one SPAA in the serving network while the pre-authentication mechanism described in this document is generally applicable to the case where there are two or more SPAA's in the serving network.

Candidate PAA (CPAA): A PAA that resides in a candidate network to which the PaC may move. A CPAA for a particular PaC may be a SPAA for another PaC.

Pre-authentication: Pre-authentication refers to EAP pre-authentication and defined as the utilization of EAP to pre-establish EAP keying material on an authenticator prior to arrival of the peer at the access network served by that authenticator [[I-D.ietf-hokey-preauth-ps](#)]. In this draft, EAP pre-authentication is performed between a PaC and a CPAA.

Pre-authorization: An authorization for a PaC, made by a CPAA for the PaC at the time of pre-authentication.

Post-authorization: An authorization for a PaC, made by a CPAA for the PaC when the CPAA becomes the SPAA for the PaC.

Pre-authorization SA: A PANA SA established between a PaC and its CPAA.

Post-authorization SA: A PANA SA established between the PaC and its SPAA.

3. Pre-authentication Procedure

A PaC that supports pre-authentication may establish a PANA session for each CPAA.

There may be several mechanisms for a PaC and a CPAA to discover each other. However, such mechanisms are out of the scope of this document.

There may be a number of criteria for CPAA selection, the timing to start pre-authentication and the timing to make a pre-authorization SA a post-authorization SA (and hence the CPAA becomes the SPAA). Such criteria can be implementation specific and thus are outside the scope of this document.

Pre-authentication may be initiated by both a PaC and a CPAA. A new 'E' (prE-authentication) bit is defined in the PANA header. When pre-authentication is performed, the 'E' (prE-authentication) bit of PANA messages are set in order to indicate whether this PANA run is for pre-authentication. Use of pre-authentication is negotiated as follows.

- o When a PaC initiates pre-authentication, it sends a PANA-Client-Initiation (PCI) message with the 'E' (prE-authentication) bit set. The PCI message MUST be unicast. The CPAA responds with a PANA-Start-Request (PSR) message with the 'S' (Start) and 'E' (prE-authentication) bits set only if it supports pre-authentication. Otherwise, it MUST silently discard the message.

- o When a CPAA initiates pre-authentication, it sends a PSR message with the 'S' (Start) and 'E' (prE-authentication) bits set. The PaC responds with a PANA-Start-Answer (PSA) message with the 'S' (Start) and 'E' (prE-authentication) bits set only if it supports pre-authentication. Otherwise, it MUST silently discard the message.
- o Once the PaC and CPAA have agreed on performing pre-authentication using the 'S' (Start) and 'E' (prE-authentication) bits, the subsequent PANA messages exchanged between them MUST have the 'E' (prE-authentication) bit set.

When a CPAA with which the PaC has a pre-authorization SA becomes the SPAA due to, e.g., movement of the PaC, the PaC performs an IP address update procedure defined in [Section 5.6 of \[RFC5191\]](#) in order to update the SPAA with the PaC's new address obtained from the new serving network. PANA-Notification-Request (PNR) and PANA-Notification-Answer (PNA) messages with 'P' (Ping) bit set are used for this purpose. The completion of the IP address update procedure will change the pre-authorization SA to a post-authorization SA. In this case, the 'E' MUST NOT be set in the PNR and PNA messages and subsequent PANA messages.

If there is another CPAA with which the PaC has a pre-authorization SA and the PaC wants to keep the pre-authorization SA after the change of SPAA, the PaC also performs an IP address update procedure defined in [Section 5.6 of \[RFC5191\]](#) in order to update the CPAA with the PaC's new address. PNR and PNA messages with 'P' (Ping) bit set is used for this purpose. In this case, the 'E' (prE-authentication) bit MUST be set in the PNR and PNA messages and subsequent PANA messages. The IP address update procedure with the CPAA will not change the pre-authorization SA to a post-authorization SA.

The pre-authorization SA and the corresponding PANA session between the PaC and a CPAA is deleted by entering the termination phase of the PANA protocol.

Example call flows for PaC-initiated pre-authentication and PAA-initiated pre-authentication are shown in Figure 1 and Figure 2, respectively.

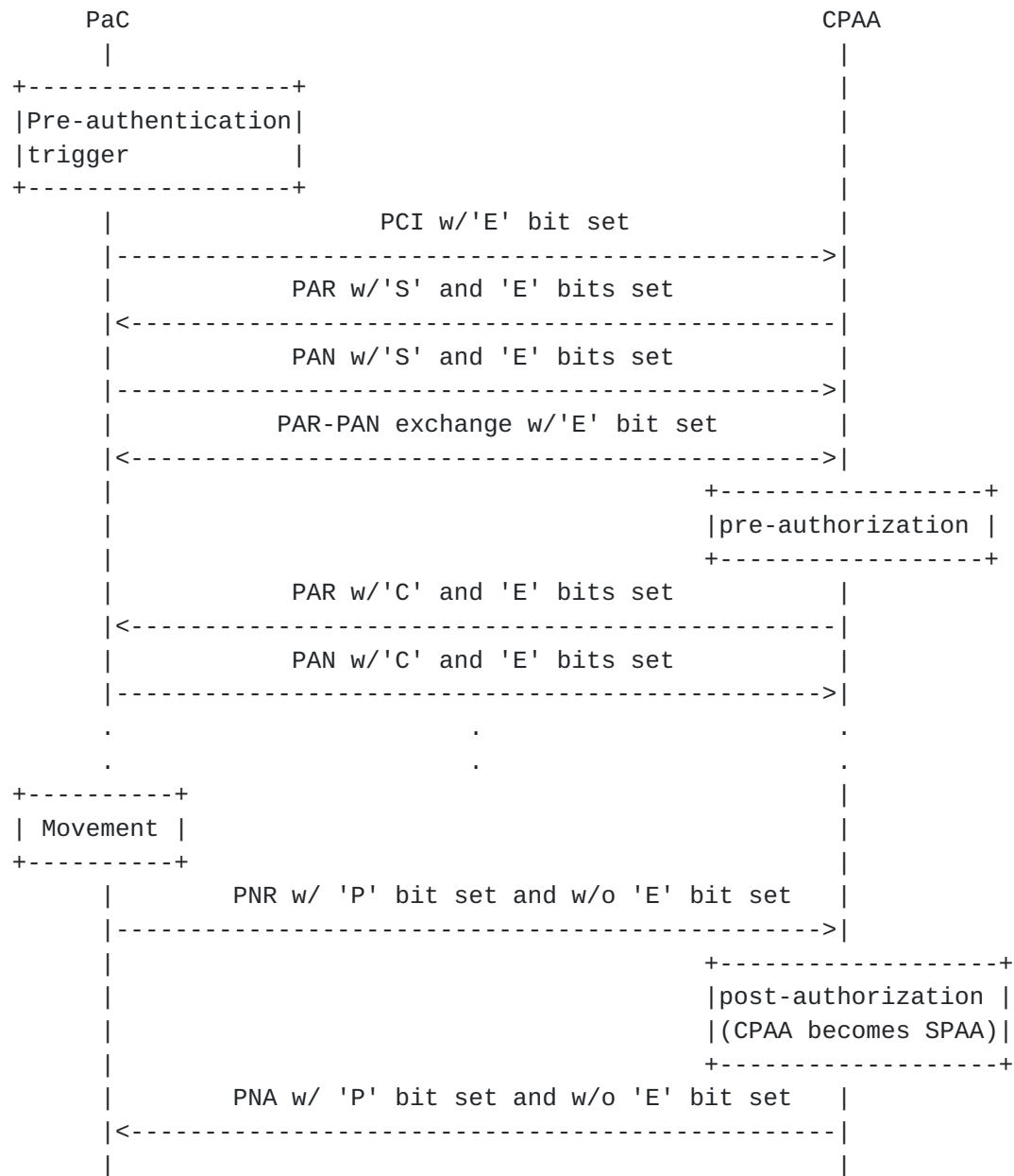


Figure 1: PaC-initiated Pre-authentication Call Flow

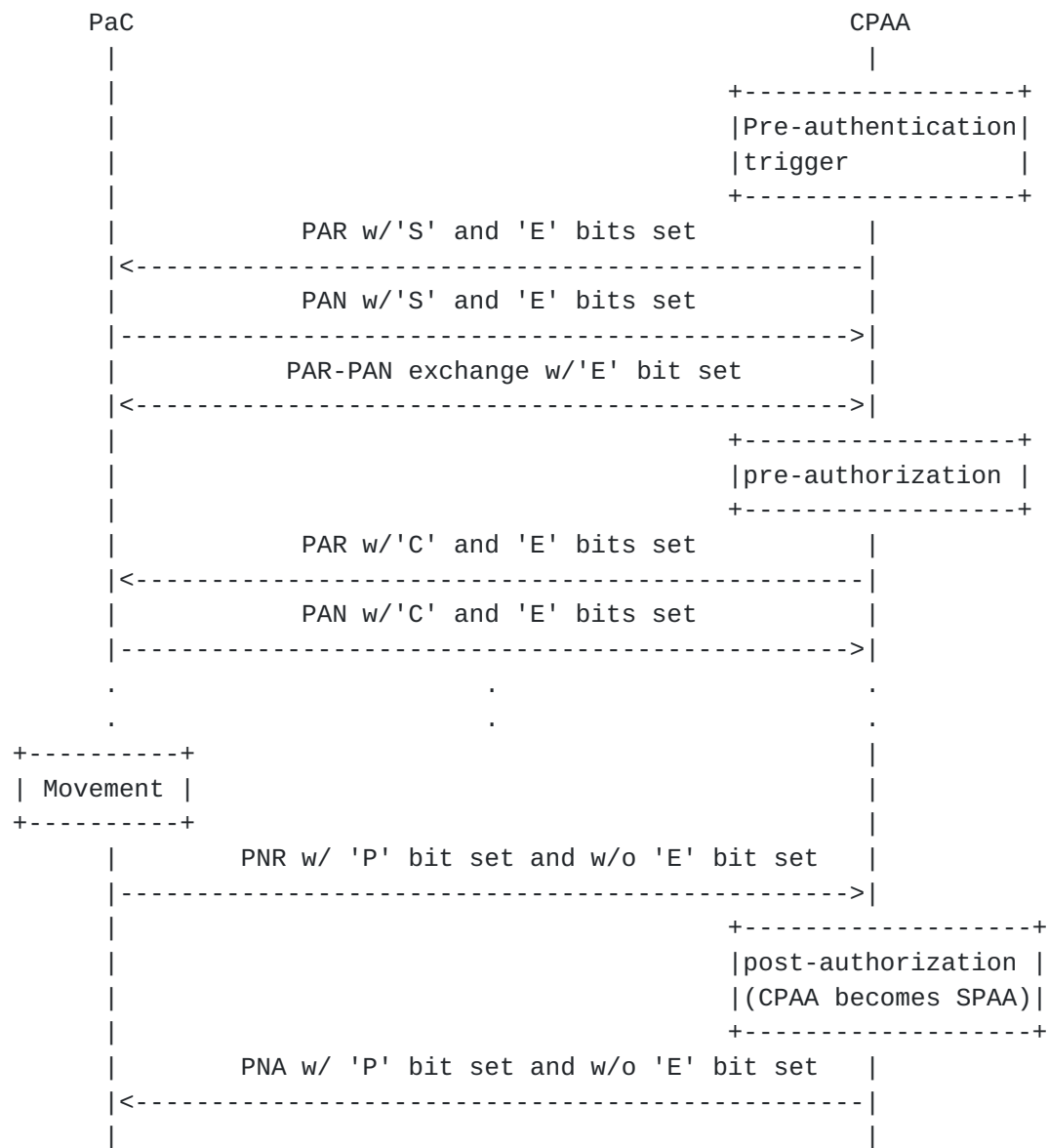


Figure 2: PAA-initiated Pre-authentication Call Flow

4. PANA Extensions

A new 'E' (prE-authentication) bit is defined in Flags field of PANA header as follows.

```

0                               1
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+---+---+---+---+---+---+---+---+
|R S C A P I E r r r r r r r r r|
+---+---+---+---+---+---+---+---+

```


E(PrE-authentication) When pre-authentication is performed, the 'E' (pre-authentication) bit of PANA messages are set in order to indicate whether this PANA run is for establishing a pre-authorization SA. The exact usage of this bit is described in [Section 3](#). This bit is to be assigned by IANA.

5. Authorization and Accounting Considerations

A pre-authorization and a post-authorization for the PaC may have different authorization policies. For example, the pre-authorization policy may not allow the PaC to send or receive packets through an Enforcement Point (EP) that is under control of the CPAA, while both the pre-authorization and post-authorization policies may allow installing credentials to the EP, where the credentials are used for establishing a security association for per-packet cryptographic filtering.

In an access network where accounting is performed, accounting starts when the pre-authorization SA becomes the post-authorization SA by default. Depending on the pre-authorization policy, accounting may start immediately after the pre-authorization SA is established.

6. Security Considerations

Since the mechanism described in this document is designed to work across multiple access networks, each EP in the serving network SHOULD be configured to allow PANA messages to be forwarded between a PaC and a CPAA only if the PaC has a post-authorization SA with the SPAA in order to avoid an unauthorized PaC to initiate pre-authentication. Also, each access network that supports pre-authentication SHOULD block pre-authentication attempts from networks from which a handover is not likely to occur.

When pre-authentication is initiated by a CPAA, it is possible that the PaC simultaneously communicates with multiple CPAAs initiating pre-authentication. In order to avoid possible resource consumption attacks on the PaC caused by a blind attacker initiating pre-authentication for the PaC by changing source addresses, the PaC SHOULD limit the maximum number of CPAAs allowed to communicate.

The pre-authentication mechanism defined in this document does not have an issue on context binding in which link-layer independent context carried over pre-authentication signaling is bound to the link-layer specific context [[I-D.ietf-hokey-preauth-ps](#)], because the same EAP transport protocol (i.e., PANA) is used for normal authentication and pre-authentication in the candidate network.

7. IANA Considerations

As described in [Section 4](#), bit 6 of the Flags field of PANA Header needs to be assigned by IANA for the 'E' (prE-authentication) bit.

8. Acknowledgments

The author would like to thank Alper Yegin, Ashutosh Dutta, Julien Bournelle and Sasikanth Bharadwaj for their valuable comments.

9. References

9.1. Normative References

[RFC5191] Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and A. Yegin, "Protocol for Carrying Authentication for Network Access (PANA)", [RFC 5191](#), May 2008.

[I-D.ietf-hokey-preauth-ps]
Ohba, Y., "EAP Pre-authentication Problem Statement",
[draft-ietf-hokey-preauth-ps-04](#) (work in progress),
September 2008.

9.2. Informative References

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

Author's Address

Yoshihiro Ohba
Toshiba America Research, Inc.
1 Telcordia Drive
Piscataway, NJ 08854
USA

Phone: +1 732 699 5305
Email: yohba@tari.toshiba.com

Full Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

