EAP Working Group
Internet-Draft
Expires: January 9, 2006

Y. Ohba
Toshiba

July 8, 2005

# Pre-authentication Support for PANA
# draft-ohba-pana-preauth-00

## Status of this Memo



## Copyright Notice



## Abstract

This document defines an extension to the PANA protocol used for proactively 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 administrative domains.

Table of Contents

## 1. Introduction

The PANA protocol [I-D.ietf-pana-pana] 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.

There is an optimization method based on Context Transfer Protocol (CTP) [I-D.ietf-seamoby-ctp] to reduce the signaling delay for establishing a PANA session with a new PAA upon a handover [I-D.ietf-pana-mobopts][I-D.bournelle-pana-ctp].

The CTP-based method have the following issues. First, it is not readily applicable to handovers across multiple administrative domains since having a security association between PAAs in different administrative domains is practically difficult. Second, even within a single administrative domain, the CTP-based method is difficult to work when the previous and new access networks have different authorization characteristics, e.g., on use of NAP and ISP separate authentication. Third, the CTP-based method relies on deriving the PANA_MAC_Key used between the PaC and the PAA in the new access network from the AAA-Key used between the PaC and the PAA in the previous access network, which does not provide perfect cryptographic separation between the PAAs.

To address the issues on the CTP-based method, this document defines an extension to the PANA protocol [I-D.ietf-pana-pana] 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 administrative domains. The proposed method is used as the authentication protocol in the framework of MPA (Media-independent Pre-authentication) [I-D.ohba-mobopts-mpa-framework].

Although the proposed method covers the case that is also covered by the CTP-based method (i.e., homogeneous authorization characteristics in a single administrative domain), the purpose of this document is not to replace the CTP-based method. Instead, the purpose of this document is to provide a way to cover the cases that are not covered by the other method. For the case covered by the CTP-based method, the CTP-based method may be used.

### 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 [I-D.ietf-pana-pana].

Access Network:

A network through which a PaC can access to the Internet via one or more EPs controlled by one or more PAAs. An access network may consist of multiple IP links.

Local PAA:

A PAA that resides in the access network where the PaC is connected. The term "local" is relative to the location of a particular PaC.

Remote PAA:

A PAA that is not a local PAA for the PaC. The term "remote" is relative to the location of a particular PaC. A PAA that is a remote PAA for one PaC may be a local PAA for another PaC.

Local PaC:

A PaC that resides in the same access network as a particular PAA. The term "local" is relative to the location of a specific PaC.

Remote PaC:

A PaC that is not a local PaC for a particular PAA. The term "remote" is relative to the location of a particular PAA. A PaC that is a remote PaC for one PAA may be a local PaC for another PAA.

Active PAA:

A local PAA for which the PaC has a PANA session.

Preparing PAA:

A remote PAA which performs pre-authentication with the PaC. A PAA that is serving as a preparing PAA for one PaC may be serving as an active PAA for another PaC.

Pre-authentication:

Authentication performed between the PaC and a preparing PAA.

Pre-authentication SA:

A PANA SA that is established between the PaC and a preparing PAA as a result of successful pre-authentication.

Active SA:

A PANA SA that is established between the PaC and an active PAA.

Pre-authorization:

An authorization that is made for the PaC by a preparing PAA as a result of successful pre-authentication.

Post-authorization:

An authorization that was made for the PaC by a PAA that was acting as a preparing PAA and has become the active PAA.

## 3. Pre-authentication Procedure

A PaC that supports pre-authentication may have one or more PANA sessions for preparing PAAs in addition to the PANA session for one of local PAAs.

There may be a number of ways to discover a remote PAA, however, remote PAA discovery and remote PaC discovery is out of the scope of this proposal.

There may be a number of criteria as to when and with which remote PAA pre-authentication is performed. 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 preparing PAA. A new flag P-flag is defined in the PANA header. When pre-authentication is performed, the P-flag of PANA messages are set in order to indicate whether this PANA run is for establishing a pre-authentication SA. Pre-authentication is negotiated in the PANA discovery and handshake phase as follows.

- When a PaC initiates pre-authentication, it sends a PANA-PAA-Discover message with the P-flag set. The PANA-PAA-Discover message MUST be unicast. The PAA responds with a PANA-Start-Request message with the P-flag set only when it supports pre-authentication. Otherwise, it MUST silently discard the message.

- When a preparing PAA initiates pre-authentication, it sends a PANA-Start-Request message with the P-flag set. The PaC responds with a PANA-Start-Answer message with the P-flag set only when it supports pre-authentication. Otherwise, it MUST silently discard the message.

- Once the PaC and preparing PAA have agreed on performing pre-authentication during the discovery and handshake phase, the subsequent PANA messages exchanged between them MUST have the P-flag set.

When the preparing PAA becomes an active PAA due to movement of the PaC, the PaC performs an IP address update procedure using PANA-Update exchange in order to update the PAA with the PaC's new address obtained from the remote network where the PAA resides. The completion of the PANA-Update procedure will change the pre-authentication SA to the active SA. The P-flag is not set in the PANA-Update messages and subsequent PANA messages.

When the PaC having an active SA with an active PAA as well as a pre-

authentication SA with a preparing PAA changes its active PAA but without changing the preparing PAA, the PaC performs an IP address update procedure using PANA-Update exchange in order to update the PAA of the PaC's new address obtained from the remote network where the new active PAA resides. The completion of the PANA-Update procedure will not change the pre-authentication SA to the active SA. The P-flag is set in the PANA-Update messages and subsequent PANA messages.

The pre-authentication SA and corresponding PANA session between the PaC and the pre-authenticated PAA can be deleted by entering the termination phase of the PANA protocol and performing the required procedure for that phase.

An example call flow for PaC-initiated pre-authentication is shown in Figure 1.

A PaC in an access network establishes a PANA session with a local PAA (l-PAA). At some point, it receives a trigger for pre-authenticating to a remote PAA (r-PAA) in another access network. The PaC then initiates a pre-authentication procedure by sending a PANA-PAA-Discover message with the P-bit set. PANA messages are exchanged between the PaC and r-PAA, with the P-bit set for all messages. On successful completion of the PANA exchanges for pre-authentication and pre-authorization, a pre-authentication SA will be established between the PaC and l-PAA. On the other hand, the active SA established between the PaC and l-PAA stays active.

At some point after establishing the pre-authentication SA, the PaC moves to the access network of the r-PAA. Then the PaC initiates a PANA-Update exchange to inform the PAA of the IP address change. In this PANA-Update exchange, the P-bit is unset. On successful completion of the PANA-Update exchange and post-authorization procedure, the pre-authentication SA becomes the active SA. The active SA between the PaC and l-PAA may stay active for a while to deal with the case in which the PaC immediately switches back to the previous access network.

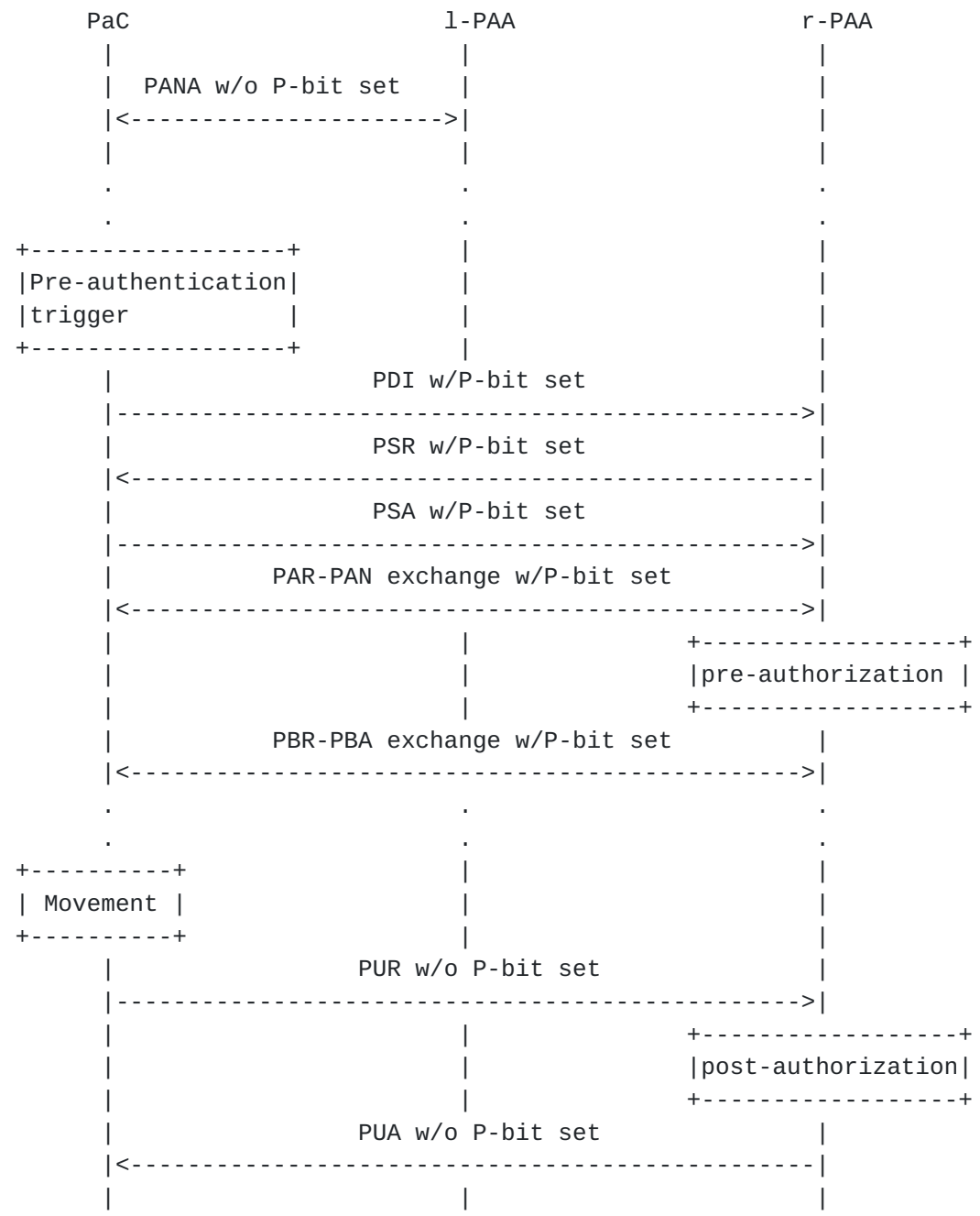



Figure 1: PaC-initiated Pre-authentication Call Flow

An example call flow for PAA-initiated pre-authentication is shown in Figure 2.

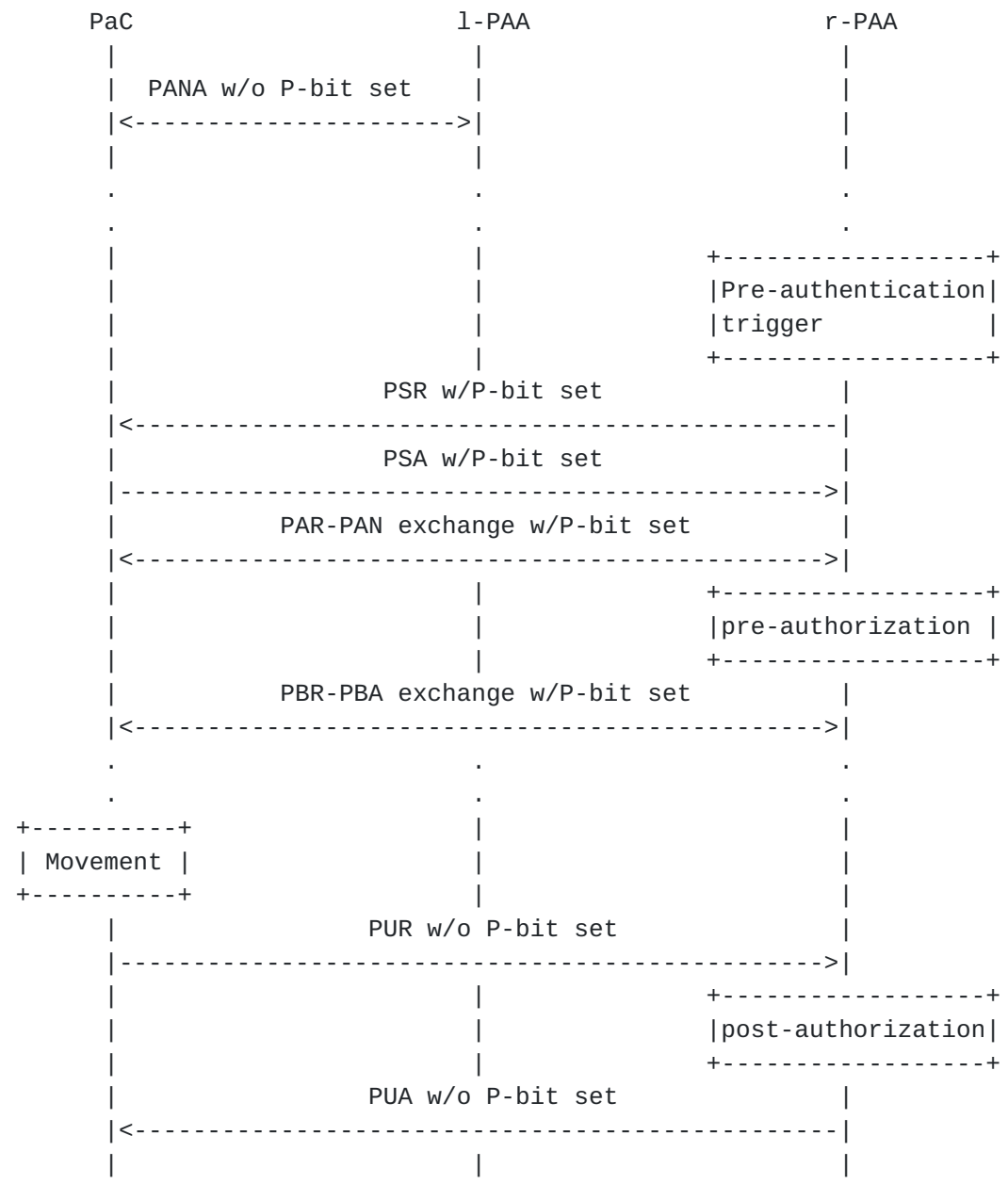
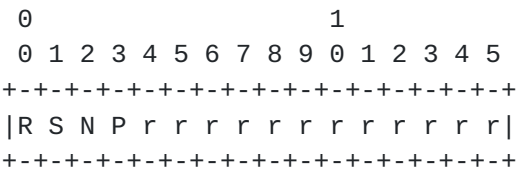



Figure 2: PAA-initiated Pre-authentication Call Flow

## 4. PANA Extensions

A new P-flag is defined in Flags field of PANA header as follows.




P(re-authentication)

When pre-authentication is performed, the P-flag of PANA messages are set in order to indicate whether this PANA run is for establishing a pre-authentication SA. The exact usage of this flag is described in Section 3. This flag 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 sent or receive packets through the EP(s) under control of the preparing PAA, while both the pre-authorization and post-authorization policies may allow installing credentials to the EP(s), where the credentials are used for establishing a security association for per-packet cryptographic filtering.

Depending on the pre-authorization policy, the PAA that has an pre-authentication SA for a PaC may start accounting immediately after the pre-authentication SA is established or may not start accounting until the pre-authentication SA becomes the active SA.

## 6. Security Considerations

Since the mechanism described in this document is designed to work across multiple access networks, each EP (Enforcement Point) SHOULD be configured to allow PANA messages to be forwarded between a PaC and a preparing PAA in a different access network only if the PaC has an active SA with a local PAA in order to avoid an unauthorized PaC to initiate pre-authentication.

When pre-authentication is initiated by a remote PAA, it is possible that the PaC simultaneously communicates with multiple remote PAAs 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 PAAs allowed to communicate.

## 7. IANA Considerations

As described in Section 4, a new flag in the Flags field of PANA Header needs to be assigned by IANA. The new flag is bit 3 ('P're-authentication).

## 8. Acknowledgments

The author would like to thank Alper Yegin and Ashutosh Dutta for their valuable comments.

## 9. References

### 9.1 Normative References

[I-D.ietf-pana-pana]
Forsberg, D., "Protocol for Carrying Authentication for Network Access (PANA)", draft-ietf-pana-pana-08 (work in progress), May 2005.

### 9.2 Informative References

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

[I-D.ohba-mobopts-mpa-framework]
Ohba, Y., "A Framework of Media-Independent Pre-Authentication (MPA)", draft-ohba-mobopts-mpa-framework-00 (work in progress), February 2005.

[I-D.ietf-pana-mobopts]
Forsberg, D., "PANA Mobility Optimizations", draft-ietf-pana-mobopts-00 (work in progress), January 2005.

[I-D.bournelle-pana-ctp]
Bournelle, J., "Use of Context Transfer Protocol (CxTP) for PANA", draft-bournelle-pana-ctp-03 (work in progress), June 2005.

[I-D.ietf-seamoby-ctp]
Loughney, J., "Context Transfer Protocol", draft-ietf-seamoby-ctp-11 (work in progress), August 2004.

## Author's Address

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

Phone: +1 732 699 5365
Email: yohba@tari.toshiba.com

## Intellectual Property Statement



## Disclaimer of Validity



## Copyright Statement



## Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.