Project	**IEEE 802.21a** **<https://mentor.ieee.org/802.21>**
Title	A Summary of Raised Issues in the Current Existing Options
DCN	**21-09-00xx-00-0Sec**
Date Submitted	**May 11, 2010**
Source(s)	Lily Chen (NIST)
Re:	Discuss at IEEE 802.21 session #37, May 10-13, 2010
Abstract	This document summarizes the raised issues in the current options for work item 1 and work item 2.
Purpose	To initial discussions on these issues at meeting #37.
Notice	This document has been prepared to assist the IEEE 802.21 Working Group. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein.
Release	The contributor grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that IEEE 802.21 may make this contribution public.
Patent Policy	The contributor is familiar with IEEE patent policy, as stated in Section 6 of the IEEE-SA Standards Board bylaws <http://standards.ieee.org/guides/bylaws/sect6-7.html#6> and in *Understanding Patent Issues During IEEE Standards Development* http://standards.ieee.org/board/pat/faq.pdf

1. INTRODUCTION

As the options in work item 1 and work item 2 were discussed in the task group, some issues were raised. This document summarizes the raised issues to initiate discussions.

2. ISSUE 1: HOW POS CAN DISTINGUISH EAP MESSAGES IN WORK ITEM 1 AND 2

In Option A of work item 1, it uses MIH to carry EAP messages between an MN and a PoS so that the PoS can forward EAP messages to a media specific authenticator (MSA) for a proactive authentication as shown in Figure 1. The MSA can be considered as a candidate attachment point (CAP) using IETF terminologies.

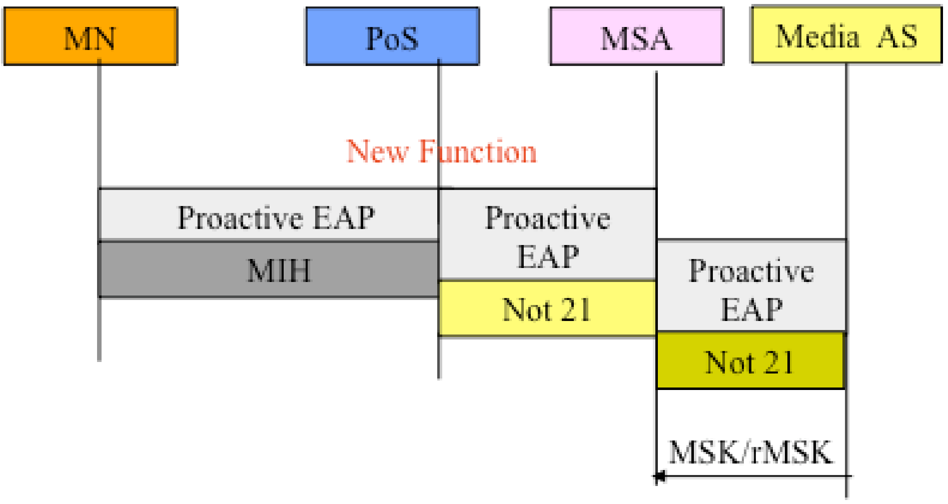

Figure 1. EAP over MIH for proactive authentication – Work Item 1.

In this case, the PoS is not an EAP authenticator. It only encapsulates and de-capsulates EAP messages using MIH message.

In Option III of work item 2, a MN executes an EAP for service access authentication with PoS as an authenticator. The EAP messages between the MN and the PoS are also carried over MIH. It can be in pass through mode with an EAP server as presented in Figure 2.

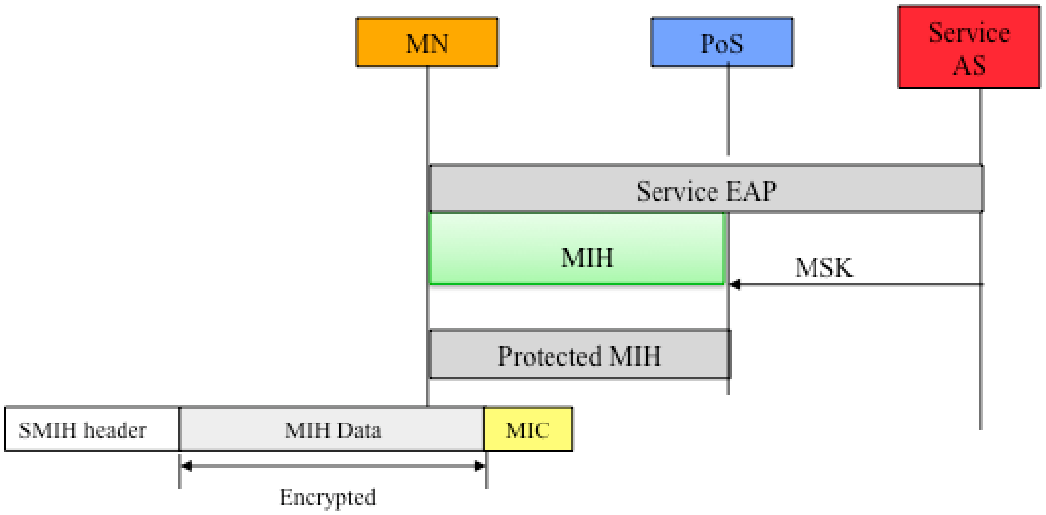

Figure 2. EAP over MIH for service authentication – work item 2

The issue is how PoS can distinguish the two situations:

1. As an authentication message routing device (do not process, only encapsulate and decapslate);
2. As an authenticator (process or pass using AAA).

Possible solutions:

1. Can we add different flags in MIH message for proactive media authentication and for service authentication?

3. ISSUE 2: AUTHENTICATOR DISCOVERY – OPTION A IN WORK ITEM 1

For option A in work item 1, in order to execute a proactive authentication, a MN may need to know which MSA should be reached. The possible situations are

1. An MN only needs to discover a PoS, while a PoS always knows which MSA the EAP messages should be forwarded to. (PoS discovery is included in 21.)
2. An MN needs to provide MSA identifier to PoS. Therefore, the MN must discover a MSA in order to execute a proactive authentication through a PoS.
3. An MN obtains a mapping table from an information server between PoSs and related MSAs.

4. ISSUE 3: POLICY VS.SECURITY CONSIDERATIONS / RECOMMENDATIONS

Currently, it is the plan to include multiple options for each work item. Some of the options, such as option 2 in work items accommodate security capability discovery and ciphersuite negotiation. The issue is how to make recommendations in 21a. There are two main opinions:

1. 21a includes some security policy so that two nodes can check whether they have agreed on a security mechanism allowed by both policies.

2. 21a includes security considerations, because 21a is not the place to specify policy.

5. NOTES

These are just some “raised” issues. More issues may appear. On the other hand, some of these issues may not be issues at all.