Project	**IEEE 802.21 MIHO** **<http://www.ieee802.org/21/>**
Title	**Resolution for Comment #2142 on Security**
Date Submitted	**March 13, 2008**
Source(s)	**Yoshihiro Ohba (Toshiba) , Subir Das (Telcordia) and Vivek Gupta (Intel Corporation)**
Re:	IEEE 802.21 Session #25 in March 2008
Abstract	This document addresses SB recirc-2 Comment #2142 on security.
Purpose	Sponsor Ballot comment resolution
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 this contribution may be made public by IEEE 802.21.
Patent Policy	The contributor is familiar with IEEE patent policy, as outlined in Section 6.3 of the IEEE-SA Standards Board Operations Manual <http://standards.ieee.org/guides/opman/sect6.html#6.3> and in *Understanding Patent Issues During IEEE Standards Development* <http://standards.ieee.org/board/pat/guide.html>.

1 Introduction

Comment #2142:

> In comment #650 on the initial ballot, I made the comment: "The draft pays lip service to security, yet a large part of the discussion within 802.11 and ongoing as part of P802.1af is concerned with optimizing the number of exchanges involved and rapidly obtaining the necessary information to re-establish prior security associations/and or make use of previously distributed keys. The separation of handoff/handover/roaming/discovery concerns from those of security is unrealistic and calls into question issues that range from the architectural placement of the handoff function to the detailed design of messages and information elements. It is completely unclear how the functions and information provided by this draft would fit within the framework of the established 802.1X

standard, the EAPOL protocol and its use of EAP, and the P802.1af amendment. Security of information transfer is required, but a major issue in handover/roaming/discovery in secured networks is determining the policy for making tentative decisions on unsecured information and confirming those decisions later." The 802.21 response to this was "The security sub-clause in section 5 has been deleted. All security related issues will be handled by the security Study Group in a future revision of the standard." I consider this response to be totally inadequate; without a clear statement in the standard of how it fits within the 802 architecture and with existing/developing security mechanisms such as 802.1X, 802.1AE, and P802.1af, I believe that the 802.21 standard will be unusable.

2 Proposed Resolution

[1] Add the following section.

5.2.3 Security design principles

The following security aspects are considered in this standard.

5.2.3.1 Relationship with 802.1 security architecture

This standard neither provides entity authentication and key establishment required for creating link-layer security associations nor requires modification to the existing link-layer ciphering schemes performed over the link-layer security associations. Instead, this standard relies on existing media-specific standards such as IEEE 802.1X and IEEE P802.1af for establishing link-layer security associations and IEEE 802.1AE for link-layer ciphering.

There are handover scenarios that are in the scope of this standard and can benefit from optimization schemes provided by IEEE P802.1af to reduce the number of exchanges involved and rapidly obtaining the necessary information to re-establish prior link-layer security associations or make use of previously distributed keys. Such scenarios include inter-technology handovers where the target access network makes use of IEEE P802.1af for peer authentication and key establishment to establish link-layer security associations. For other handover scenarios, other mechanism such as the EAP (Extensible Authentication Protocol) extensions for EAP re-authentication protocol defined in IETF can be used to reduce the number of EAP message exchanges for establishing link-layer security associations if the target link-layer technology supports the EAP extensions.

5.2.3.2 MIH protocol security

This standard does not provide the MIH protocol with security properties such as entity authentication, message authentication and replay protection, and confidentiality required for securing the MIH protocol. Instead, this standard relies on MIH transport protocols to

provide these security properties to secure the MIH protocol. In order for the MIH protocol to make use of entity authentication provided by an MIH transport protocol, the MIHF identifiers of the two MIH peers need to be used as the identifiers for entity authentication required for establishing an MIH transport protocol security association between them. In the case where the security properties are not provided by an MIH transport protocol, e.g., media-independent information service over unprotected link-layer management frames, the MIH protocol messages are not secured, and it would be up to the policy decision entity to prepare for handover based on the information obtained from the unsecured MIH protocol exchanges. At a later stage, after associating with the target point of attachment, the same information can be verified with the use of MIH transport protocol security.

[2] Add the following informative references in Annex J:

IEEE Standards for Local and metropolitan area networks—Port-Based Network Access Control.

IEEE P802.1X-REV/D2.0 Draft Standard for Local and Metropolitan Area Networks—
Port-based Network Access Control.

IEEE Std 802.1AE™-2006 IEEE Standard for Local and metropolitan area networks Media Access Control (MAC) Security.

IETF Internet Draft (draft-ietf-hokey-erx-13.txt, 2008-02), EAP Extensions for EAP Re-authentication Protocol (ERP).