Draft PAR Confirmation Number
Submittal Email: vivekggupta@ieee.org
Type of Project: "Amendment to Existing Standard"
1.1 Project Number: P802.21a
1.2 Type of Document: Standard for
1.3 Life Cycle: Full
1.4 Is this project in ballot now? No
2.1 Title of Standard: Standard for Local and Metropolitan Area Networks: Media Independent Handover Services - Security Extensions to Media Independent Handover Services and Protocol
3.1 Name of Working Group: Media Independent Handoff Working Group(C/LM/WG802.21) **Contact information for Working Group Chair** Vivek Gupta 4945 Bridgeview Lane, San Jose, CA 95138 US, vivekggupta@ieee.org **Working Group Vice Chair:** Subir Das One Telcordia Drive Piscataway, NJ 08854 US, **Email:** subir@research.telcordia.com
3.2 Sponsoring Society and Committee:IEEE Computer Society/Local and Metropolitan Area Networks(C/LM) **Contact information for Sponsor Chair:** Paul Nikolich 18 Bishops Lane Lynnfield, MA 01940 US p.nikolich@ieee.org **Contact information for Standards Representative:**
4.1 Type of Ballot: Individual
4.2 Expected Date of Submission for Initial Sponsor Ballot: 2010-11
4.3 Projected Completion Date for Submittal to RevCom: 2011-08
5.1 Approximate number of people expected to work on this project: 30
5.2 Scope of Proposed Standard:

- Define mechanisms to reduce the latency of authentication and key establishment signaling for handovers between access networks that support IEEE 802.21.
- Define mechanisms that provide data integrity, replay protection, confidentiality and data origin authentication to IEEE 802.21 MIH (Media-Independent Handover) protocol exchanges. Define mechanisms to enable authorization for MIH services

5.3 Is the completion of this standard is dependent upon the completion of another standard: No
If yes, please explain:

5.4 Purpose of Proposed Standard:

The purpose of this amendment is to (i) reduce the latency of authentication and key establishment signaling for handovers between heterogeneous access networks and (ii) secure MIH protocol exchanges and enable authorization for MIH services.

5.5 Need for the Project:

- It is essential to reduce the latency of authentication and key establishment signaling to realize session continuity for real-time applications. This is especially true in handover scenarios wherein the mobile node disconnects its active connection with the serving access network before making another connection with the target access network.
- Security of MIH protocol currently relies on the security of the underlying transport protocols without a mechanism to authenticate peer MIH entities. This lack of authentication of peer MIH entities does not provide proper authorization for MIH services. As such it is required to secure the MIH protocol and develop mechanisms to authenticate peer MIH entities.

5.6 Stakeholders for the Standard: Semiconductor manufacturers, mobile and wireless device manufacturers and network operators.

Intellectual Property
6.1.a. Has the IEEE-SA policy on intellectual property been presented to those responsible for preparing/submitting this PAR prior to the PAR submittal to the IEEE-SA Standards Board? Yes
If yes, state date: 2008-05-12
If no, please explain:
6.1.b. Is the Sponsor aware of any copyright permissions needed for this project? No
If yes, please explain:
6.1.c. Is the Sponsor aware of possible registration activity related to this project? No
If yes, please explain:

7.1 Are there other standards or projects with a similar scope? No
Explanation:
Sponsor Organization:
Project/Standard Number:
Project/Standard Date: 0000-00-00
Project/Standard Title:

7.2 International Standards Activities

a. Adoptions

Is there potential for this standard to be adopted by another organization? No
Organization:
Technical Committee Name:
Technical Committee Number:
Contact person Name:
Contact Phone:
Contact Email:

b. Joint Development

Is it the intent to develop this document jointly with another organization? No
Organization:
Technical Committee Name:
Technical Committee Number:
Contact person Name:
Contact Phone:
Contact Email:

c. Harmonization

Are you aware of another organization that may be interested in portions of this document in their standardization development efforts? No
Organization:
Technical Committee Name:
Technical Committee Number:
Contact person Name:
Contact Phone:
Contact Email:

8.1 Additional Explanatory Notes: (Item Number and Explanation)

CRITERIA FOR STANDARDS DEVELOPMENT (FIVE CRITERIA)

Broad Market Potential

A standards project authorized by IEEE 802 shall have a broad market potential. Specifically, it shall have the potential for:

a) Broad sets of applicability.
b) Multiple vendors and numerous users.
c) Balanced costs (LAN versus attached stations).

IEEE 802.21 defines MIH (media-independent handover) services that facilitate handover optimization between heterogeneous access networks including IEEE 802 access technologies and other access technologies. Therefore, IEEE 802.21 is applicable to network service providers as well as equipment vendors.

There is a wide variety of vendors currently building numerous wired and wireless products for the network equipment market segments. Many vendors, and others, participated in the standard development process of IEEE 802.21.

Currently, security mechanisms, including authentication and key establishment have been specified for each access technology. During a handover from one access technology to another, authentication and key establishment will introduce latency to establish a new security association between the mobile node and the target network. Reducing this latency will assure service continuity during handovers.

The MIH services can be a new target to attackers, which will be the main concerns for equipment vendors and service providers. Service protection based on cryptographically binding of MIH services to authenticated service entities will prevent from attacks that can potentially paralyze the network.

Compatibility

IEEE 802 defines a family of standards. All standards shall be in conformance with the IEEE 802.1 Architecture, Management and Interworking documents as follows: 802. Overview and Architecture, 802.1D, 802.1Q and parts of 802.1f. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with 802.
Each standard in the IEEE 802 family of standards shall include a definition of managed objects which are compatible with systems management standards.

1. The proposed project will be developed in conformance with the IEEE 802 Overview and Architecture.
2. Managed objects will be defined consistent with existing policies and practices for IEEE 802.1.

Consideration will be made to ensure that compatibility is maintained with IEEE 802 security mechanisms and that existing security mechanisms are not compromised.

Distinct Identity

Each IEEE 802 standard shall have a distinct identity. To achieve this, each authorized project shall be:
a) Substantially different from other IEEE 802 standards.
b) One unique solution per problem (not two solutions to a problem).
c) Easy for the document reader to select the relevant specification.

1. There is no IEEE 802 standard to reduce latency caused by authentication and key establishment for handovers between heterogeneous access networks. There is work in progress in IETF (Internet Engineering Task Force) to support optimization for authentication and key establishment during handovers by extending Extensible

Authentication Protocol (EAP) to support low-latency re-authentication. However this effort is not addressing issues which are dependent on L2 access networks. Authentication and key establishment need to be performed as proactively as possible to reduce the overall security signaling latency instead of performing the same procedure after the mobile node attaches to the target network.

2. There is no IEEE 802 standard to provide data integrity, replay protection, confidentiality and data origin authentication for MIH protocol exchanges.

Technical Feasibility

For a project to be authorized, it shall be able to show its technical feasibility. At a minimum, the proposed project shall show:

a) Demonstrated system feasibility.
b) Proven technology, reasonable testing.
c) Confidence in reliability

1. Security mechanisms including data integrity, replay protection, confidentiality and data origin authentication, have been applied to different media types.

   Some authentication protocols have been commonly adopted by different media, e.g. EAP. Media independent key hierarchy and an optimized authentication mechanism based on EAP are under development in IETF. Additional optimization mechanisms are required for proactively performing authentication and key establishment signaling between a mobile node and an authenticator in the target network via the serving network. This can be defined as an extension to IEEE 802.21 with the use of EAP.

   Once a link layer security association is created between the mobile node and the target point of attachment, the existing algorithms defined for the target link layer can be used to provide data integrity, replay protection and confidentiality.
2. There are security mechanisms provided by MIH transport protocols. It is possible to use existing transport security mechanisms once a mechanism to bind the identities of authenticated MIH entities to the transport security mechanisms is defined.

Economic Feasibility

For a project to be authorized, it shall be able to show economic feasibility (so far as can reasonably be estimated), for its intended applications. At a minimum, the proposed project shall show:
a) Known cost factors, reliable data.
b) Reasonable cost for performance.
c) Consideration of installation costs.

Handover procedures with security have been implemented within each access technology. Existing deployment of cellular and IEEE 802 access technologies provide real world examples of secured handover mechanisms within homogeneous networks at layers 1 and 2 (PHY and MAC). These have been proven to be cost effective solutions.

The features to be defined in this project will reduce the latency caused by authentication and key establishment during inter-technology handovers. The features to be defined in this project also provide data integrity, replay protection, confidentiality and data origin authentication to MIH protocol message exchanges. These represent a marginal increment to the cost of existing networking devices and do not represent an originating cost.