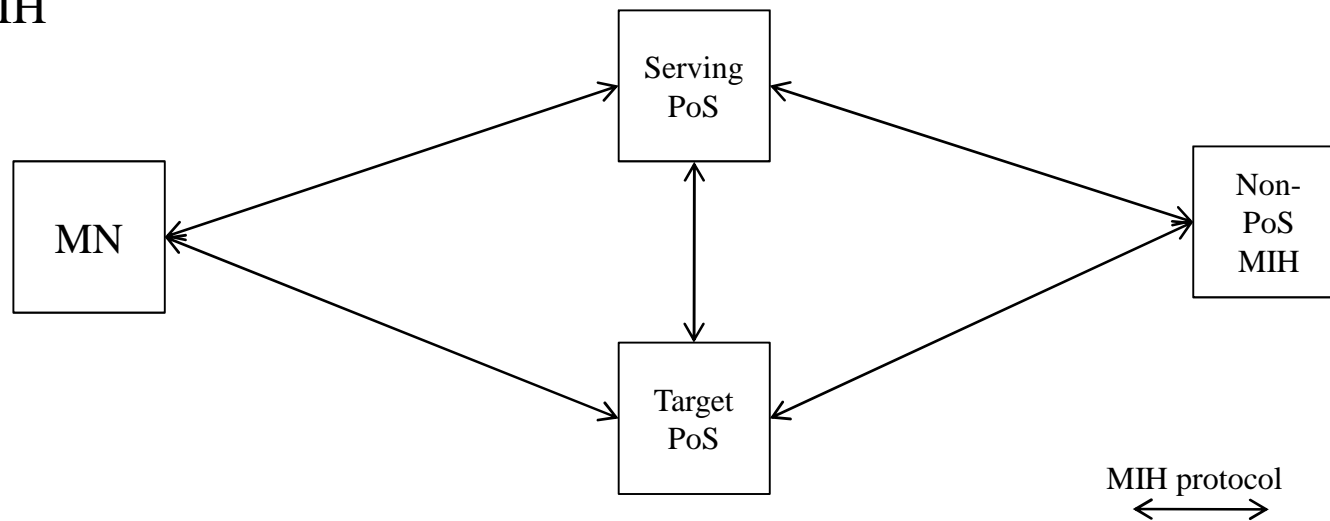


IEEE 802.21a Status Report

Yoshihiro Ohba

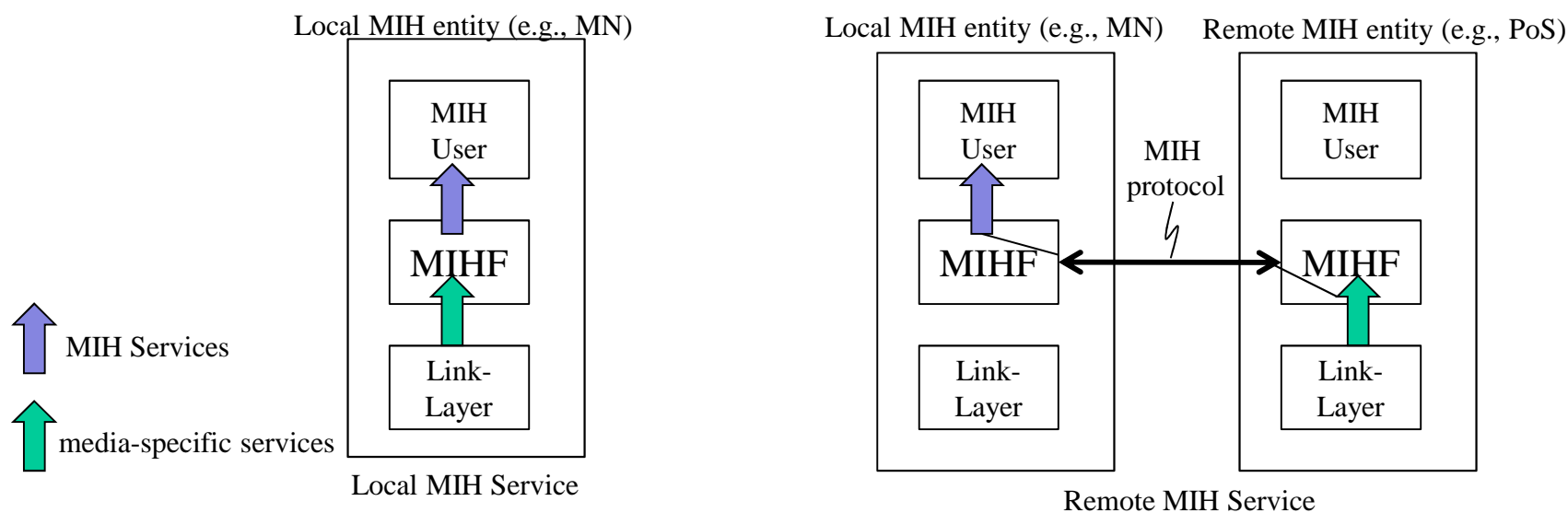
What is IEEE 802.21?

- IEEE 802.21 is a standard for Media-Independent Handover (MIH) services
- MIH services are defined to facilitate handovers between heterogeneous networks
 - Handovers between networks with different access technologies
 - Handovers between 802.11 networks with different ESS's (Extended Service Sets)
- MIH Services: Event Service (ES), Command Service (CS), Information Service (IS)
- MIH Protocol entities : Mobile Node (MN), Point of Service (PoS), Non-PoS MIH



MIH Protocol

- Remote MIH services are provided on top of MIH protocol
- MIH protocol runs between MIH Functions (MIHFs) of different MIH entities
- MIH protocol is defined to work over L2 or L3
 - MIH over Ethernet : defined in IEEE 802.21
 - MIH over 802.11: defined in IEEE 802.11u
 - MIH over 802.16: defined in IEEE 802.16g, 802.16m
 - MIH over TCP and UDP: defined in RFC 5677
- Security of MIH protocol is currently under development



What is IEEE 802.21a?

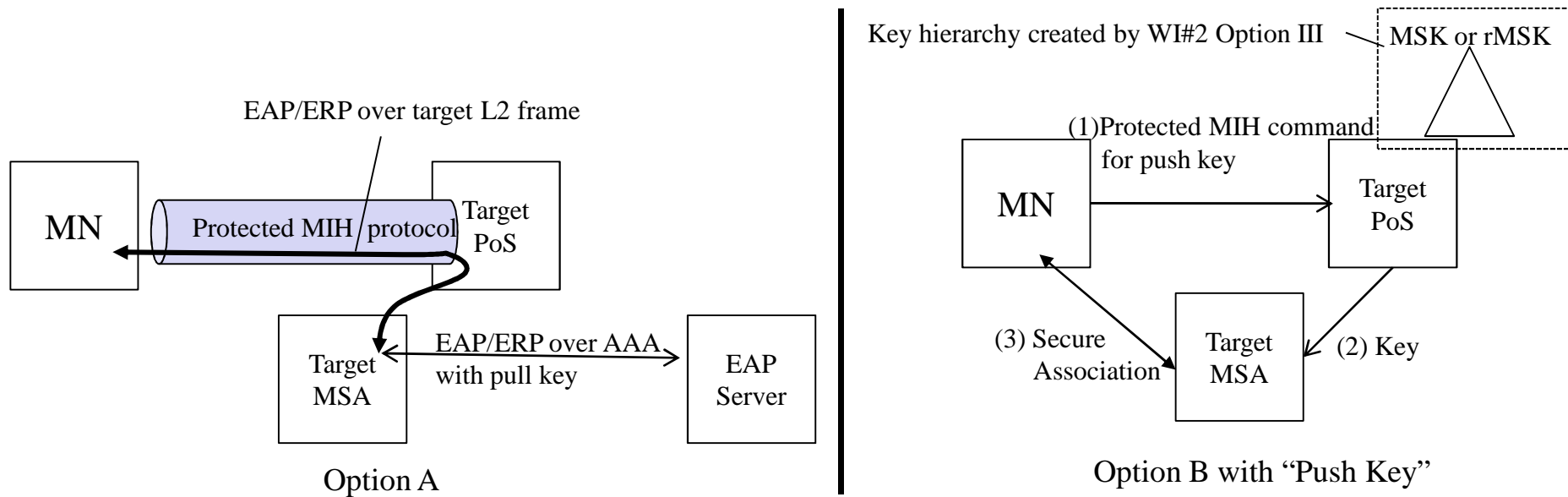
- Standard for Local and Metropolitan Area Networks: Media Independent Handover (**MIH**) Services - Amendment for Security Extensions to Media Independent Handover Services and Protocol
- Two work items in IEEE 802.21a:
 - <http://mentor.ieee.org/802.21/file/09/21-09-0010-00-0sec-p802-21a-par.pdf>
 - “This standard defines mechanisms
 - (i) to reduce the latency during authentication and key establishment for handovers between heterogeneous access networks that support IEEE 802.21
 - (ii) to provide data integrity, replay protection, confidentiality and data origin authentication to IEEE 802.21 MIH (Media-Independent Handover) protocol exchanges and enable authorization for MIH services.”

Proposals for Work Item #2

- Option I: Protection provided by MIH transport protocol
- Option II: Protection within MIH protocol using (D)TLS over MIH for authentication, key establishment and ciphering
- Option III: Protection within MIH protocol using MIH-specific ciphering
 - EAP or ERP over MIH is used for service authentication and key establishment for MIH

Proposals for Work Item #1

- Option A: A proactive authentication scheme to carry out EAP or ERP between MN and target MSA (Media-Specific Authenticator) through target PoS
 - MIH protocol tunnels EAP over target L2
 - Similar to direct pre-authentication
 - Also defines some Information Elements to discover candidate PoS and MSA
- Option B: A proactive authentication scheme that utilizes a key hierarchy generated from EAP or ERP over MIH defined in WI#2 option III
 - Three key distribution schemes are defined to carry keys under the key hierarchy from target PoS to target MSA, i.e., push key, reactive pull key, and proactive pull key



802.21a Project Timeline

	Y2009						Y2010						Y2011					
	1	3	5	7	9	11	1	3	5	7	9	11	1	3	5	7	9	11
Call for Proposals		x																
Proposal presentatiuon & harmonization			x	x	x	x	x	x	x									
Down-selection										x								
Letter Ballot											x	x						
Sponsor Ballot													x	x	x	x		
Specification sent to RevCom																	x	

- Status as of now
 - Completed down-selection on July, 2010
 - All options have been accepted
 - A draft specification is under development

Thank You!