

IEEE P802.21 Media Independent Handover Services

Teleconference Minutes of the IEEE P802.21a Security Task Group

Chair: Yoshihiro Ohba

Editor: Lily Chen

Minutes taken by Lily Chen

Date: June 22, 2010, 9:00 am -11:00 am, US EDST

Chair called the teleconference to order, reminded the IEEE-SA patent policy and introduced the participants:

List of Participants:

Subir Das (Telcordia)

Lily Chen (NIST)

Yoshihiro Ohba (Toshiba Corporation)

Rafael Marin-Lopez (University of Murcia).

Fernando Bernal-Hidalgo (University of Murcia)

**Chair** called the teleconference to order and introduced the participants. Also reminded the IEEE SA patent and policy procedures.

The proposal 21-10-0120-00-0sec is presented at the teleconference. Rafael Marin-Lopez was the presenter. The presentation provides a summary of option III for work item 2 specified in 21-10-0078-03-0sec. The option III in work item 2 includes a MIH service authentication using EAP and key establishment for MIH protections. This option is also related to option B of work item 1, which bundles media access authentication with service authentication. In that case, the procedure described in this proposal also establishes and distributes keys for media authentication.

**Q**: On page 5, in negotiation stage, why 4 messages are needed? In negotiation stage, MIH\_Auth\_request is sent from both MN and PoS. Are these two sets of messages necessaryA: Yes, we can reduce it into two messages.

Comment: Instead of defining new negotiation message, we should use the capability discovery message. This way we will avoid defining new primitives.

**A**:. We can use capability discovery. But we do not know which option is better.

**Q**: Why the messages for negotiation stage used in page 11 are different from the messages on page 5?

**A**: We can use flags to distinguish the messages used in the different stages or we can use different commands. In MIH message header, a 4-bit field can be used as a flag.

**Q**: I tend to think define less new messages is better. Can we use capability discovery message? If we can, we only need to define new IEs and/or add new parameters to the primitives.

**A**: That is an option.

**Comment**: It seems that using capability discovery is better.

**A**: Capability discovery needs to be bound with authentication. We will take a look to see if we need to define some new TLVs to include within the capability discovery.

**Q**: In the defined authentication messages, is ERP included?

**A**: Yes. This is captured in the key hierarchy. After the authentication, it can generate MSK or a rMSK.

**Q**: We probably need to include ERP messages explicitly.

**A**: The slides are trying to describe a general case.

**Q**: In negotiation stage, is the cipher suite for protecting EAP messages also negotiated?

**A**: No. The EAP message protection algorithms will be negotiated by EAP. The algorithms used to protect MIH are negotiated in negotiation stage.

**Q**: If encryption is enabled, shall it be mandatory? Do we give alternatives?

**A**: Encryption can be an option, if the service is provided for free. However, if the service is provided in a subscription based, then encryption may be needed since some one may steal the information service through eavesdropping. On the other hand, if the service is free, then the only reason to encrypt is to provide privacy. It does seem privacy is an issue for the MIH service.

**Q**: Can encryption be negotiated?

**A**: Yes. It can. Null encryption can be an option.

**Q**: On page 8, is encryption is enabled, is MIH header encrypted?

**A**: Only MIH data is encrypted. I do not see any reason to encrypt the header.

**Q**: The header may include some identifiers.

**A**: In IPsec, ESP does not encrypt the IP header, just payload. Why should we? Are you thinking about privacy?

**Q**: Yes. MIHF-ID may need to be protected?

**A**: Why?

**Q**: To provide identity privacy.

**A**: I do not know whether we need to provide privacy.

**Q**: Do we have to deal with privacy? Is MIHF-ID related to a user?

**A**: We did not see any requirement.

**Comments**: We can check the requirements for 21a.

**Presenter**: On page 10, 6 commands are defined. The first 4 commands are used purely for MIH authentication. If we use capability discovery, we may only need 3 commands among the 4 commands.

On page 11, if we use capability discovery, we need to modify the messages.

**Q**: Does a PoS need to know where to distribute the keys?

**A**: Yes, it needs to know which MSA.

**Q**: Does a PoS need to know the option for key distribution?

**A**: A PoS needs to know the key distribution option only in bundle case.

**Presenter**: The MIH service authentication defined here can be a proactive authentication.

**Q**: We know what it means in media authentication case. How it is defined in service case?

**A**: When an MN is not in the PoS’s domain, it can execute a proactive service authentication. We have two options, proactive or non-proactive. We can use a flag to distinguish these two cases.

**Comment**: I think it makes sense.

**Presenter**: On page 17, we described finalize phase.

**Presenter**: In the authenticated/authorized phase, we can negotiate push or pull key distribution for bundled case. This is considered as a service to a MN.

**Q**: Which service is this?

**A**: Command service.

**Q**: On page 13, is it true that message 2 and 3 are not MIH messages.

**A**: Yes.

**Q**: I see a difference between page 13 and page 14. On page 13, the MIH user in PoS is not involved, while on page 14, MIH user in PoS is involved. Can you explain?

**A**: This is because we do not know whether MIHF can handle message 4 and 5 on page 14. If it can, then we do not need to involve MIH user. Any comments?

**Q**: On page 13, it seems like MIH user can handle messages 2 and 3.

**Presenter**: On page 14, message 3, it should include link layer frames. This is related to Dapeng’s proposal. We have sent an e-mail to Dapeng to synchronize. We haven’t received any reply yet. In our case, the message is protected through MIH protection. But in work item 1, the message is only protected at layer 2. We need to discuss with Dapeng.

**Q**: On page 16, is it true that we do not need to define any MIH new messages for key distribution?

**A**: That is correct.

**Q**: Can you elaborate “another issue” on page 18?

**A**: We have considered two cases to cover: whether a PoS is or is not collocated with a PoA. Therefore, it is more likely an IEEE 802 technology will use a .21 entity PoS, compared to other entities such as PANA agent.

**Comment**: That is a good point. WiMax has .21 features included currently. It shows that 21 is more applicable to IEEE 802 technologies.