

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 Yoshihiro Ohba

Date: August 17, 2010, 9:10 am -11:10 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)

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

# Chair mentioned the following documents as agenda items: 21-10-0170-00 (Comments on option II of work item #2) and 21-10-0169-00 (Option for Security IEs). The agenda is unanimously approved.

# Discussion on DCN 21-10-0170-00

There was a comment that DCN 21-10-171-00 addresses comments described in 21-01-0170-00. Therefore DCN 21-10-171-00 is presented as part of 21-10-0170-00 discussion. Each comment in DCN 21-10-171-00 was reviewed one by one.

## Comment LLC1

It was suggested to delete the earlier text (referred in LLC1) and modify the latter text (referred in LLC3) to maintain consistency. (D)TLS credentials may be based on a PSK or a certificate.

## Comment LLC4

When to use TLS or DTLS depends on reliability of MIH transport. If MIH transport is TCP use TLS. If MIH transport is UDP, use DTLS.

## Comment LLC5

Mapping between transport address and MIHF ID is maintained through Session ID TLV. While there are other ways of maintaining the mapping (e.g., carrying MIHF ID in every MIH message), this is an optimized way of dealing with change of transport address.

Question: Do we need to explain this advantage?

Answer: Yes, the current text is not self-explanatory.

## Comment LLC6

Comment: MIH SA is not well defined.

Comment: MIH SA will be clearly defined in consultation with the contributors of Work Item #2 Option III to cover both protection methods at MIH layer (i.e., TLS-based protection and MIH-specific protection).

Comment: MIHF has to use the respective algorithms and policies corresponding to the negotiated MIH SA over MIH layer.

Comment: In the case of TLS-based protection over MIH, encryption and integrity is provided by TLS record layer, but it is integral part of MIH protocol security.

Comment: After TLS handshake, we have upper MIH layer and lower MIH layer. Before or during TLS handshake, it is not sure whether there is lower MIH layer only or upper MIH layer only.

Comment: It will be confusing if we describe based on upper and lower MIH layers as it depends on the format of TLS-based MIH protocol protection.

Comment: We also need to change MIHS header format not to use Service ID to indicate security. We may have to use one-bit in some other field to indicate security.

## Comment LLC7

Comment: We use TLS record layer to protect MIH PDU.

Question: Is MIHS header still needed if MIH PDU is contained in TLS TLV?

Answer: Yes, MIHS security header is needed to indicate that there is MIH security. This clarification also addresses LLC8, LLC9, LLC10 and LLC11.

# Discussion on DCN 0169 was postponed due to absence of the main contributor related to Work Item #1 Option A.