 

IEEE P802.21.1 Media Independent Services and Use Cases

Meeting Minutes of the IEEE P802.21m Task Group

Chair: Subir Das

# Meeting Minutes of the IEEE P802.21m Task Group Teleconference

## Monday, August 02, 2015 (8:00-9:00 AM, US EDT)

Participants:

Yoshikazu Hanatani ( Toshiba)

Yusuke Shimizu (Panasonic)

Hyeong Ho Lee (ETRI)

Lily Chen (NIST)

Subir Das (ACS)

Meeting called to order by Chair at 8:05 AM

Chair read the rules and reminded the patent policies.

No LOA was declared.

Chair mentioned that he contacted IEEE-SA editor for getting consolidated IEEE 802.21d in the revision draft. IEEE-SA will try her best to provide an update before September Interim meeting although they are extremely busy.

Yoshikazu Hanatani presented Draft for changing AES-CCM in the GKB-generated MIH SA.

He addressed the comments that were received in Jul Plenary meeting.

The associated data, A, not to be encrypted but authenticated is formed by concatenating the MIH Header, the Source MIHF Identifier TLV, the Destination MIHF Identifier TLV as presented in MIH PDU and the SAID TLV with padding

Q: Omitting the digital signature and introducing the associated data, outsider attack can be mitigated but the insider threat still exists, correct?

A: Yes

Comment: We should add some clarification texts in the background section.

Authors will update the draft accordingly.

Q: Can we split the sentence of associated data definition?

A: Yes, it will be done.

Q: In section 9.6.3.1 bullet d), it is ok to delete “not to be encrypted”. Same is true for c), ‘to be encrypted’

A: It will be updated.

Q: Why do we need two octets?

A: Since we need one for group key distribution for protecting the payload data and another one for group key distribution for generating the group key.

Call ended at 8:44 am