

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 31, 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:

Rafa Marin Lopez (University of Murcia)

Fernando Bernal (University of Murcia)

Lily Chen (NIST)

Dapeng Liu (China Mobile)

Yoshihiro Ohba (Toshiba Corporation)

Subir Das (Telcordia)

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

1. Chair made condolence statement about Ms. Yuu-Heng Alice Cheng who passed away on August 14th. Alice served as Secretary of 802.21 Security SG before the 802.21a TG was formed and helped the SG a lot.

# Chair mentioned the following documents as agenda items: 21-10-0078-03 and 21-00-0120-03 (Comments on option II of work item #2) and 21-10-0169-00 (Option for Security IEs). The agenda is unanimously approved.

# Discussion on 21-10-0078-03 and 21-00-0120-03

* 1. Discussion on Comments LLC1, LLC2 and LLC3

PRF+ currently uses feedback, which is ok. It is suggested to use HMAC-based Extract-and-Expand Key Derivation Function (HKDF) RFC 5869 for more formal definition of PRF+.

Comment: What is PRF+ and KDF?

Comment: PRF+ is KDF.

Comment: Do not use different names to mean the same thing. Let’s use one word.

* 1. Discussion on Comment LLC4

Random numbers are carried in MIH\_Auth messages.

* 1. Discussion on Comment LLC11

The parameters (identifiers, key distribution mechanisms and ciphersuites) have been included in the different primitives.See sections from 2.6.1.3 to 2.6.1.6 in the document.

* 1. Discussion on Comment LLC6

Same random numbers are used for generating MIIK and MIEK.

Comment: When generating child keys you don’t know which algorithm will be used and how long the key length will be.

Comment: negotiation needs to be performed before authentication and the negotiation is unprotected. Keys will not be generated until negotiation is done.

* 1. Discussion on Comment LLC9

List of algorithms are listed.

Comment: Some of them are not NIST-approved. Want to narrowdown.

Comment: Suggest Rafa and Lily to work together to narrowdown the ciphersuites.

* 1. Discussion on Comment LLC10

Detailed description on packet processing is provided now.

Comment AEC-CCM may need more, for example how nonce is carried. NIST 800-38C. Yoshi will check 800-38C to see what is needed in 802.21a.

Comment: Header format needs to be revised to support both options ii and iii ciphering.

Comment: We need to define how to know the packet is protected and how from the MIH header.

* 1. Discussion on Comment LLC6 (in slide #10 and #11)

MS-ROOT key is defined between MSK/rMSK and MS-PMKs.

* 1. Discussion on Comment LLC12/13

Messages that are not part of 802.21a are represented differently

# Discussion on DCN 21-10-0169. There are two ways to carry security related IEs. We need to choose one way.

# Comment: Option-1 is better because it’s quite natural and simple.

# Additional discussion on capability discovery and ciphersuite negotiation in relation to DCN 21-10-0078-03.

Comment: Capability discovery should not be used for parameter negotiation, otherwise PoS will need to maintain state for a large number of MNs regardless of their capabilities

# Document submission deadline for revised proposal is September 7, 2010.

1. The teleconference ended at 11:18am