IEEE P802.11  
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Security related requirements for Specification Frame Work Document | | | | | | | | | |
| Date: 2012-03-12 | | | | | | | | | |
| Author(s): | | | | | | | | | |
| Name | Affiliation | | Address | | | Phone | | email | |
| George Cherian  Santosh Abraham  Jouni Malinen | | Qualcomm | | 5775 Morehouse Dr., San Diego, CA | 8586516645 | | gcherian@qualcomm.com | |
| Hitoshi MORIOKA | | Allied Telesis R&D Center. | | 2-14-38 Tenjin, Chuo-ku, Fukuoka 810-0001 JAPAN | +81-92-771-7630 | | hmorioka@root-hq.com | |
| Hiroshi Mano | | Allied Telesis R&D Center. | | 7-21-11 Nishi-Gotanda, Shinagawa-ku, Tokyo 141-0031 JAPAN | +81-3-5719-7630 | | hmano@root-hq.com | |
| Mark RISON | | CSR | | Cambridge Business Park, Cowley Road, Cambridge CB4 0WZ UK | +44-1223-692000 | | Mark.Rison@csr.com | |
| Marc Emmelmann | | Fraunhofer FOKUS | | Kaiserin-Augusta-Alle 31 10589 Berlin Germany | +49-30-3463-7268 | | emmelmann@ieee.org | |
| Ping Fang | | Huawei Technologies Co., Ltd. | | Bldg 7, Vision Software Park, Road Gaoxin Sourth 9, Nanshan District, Shenzhen, Guangdong, China, 518057 | +86 755 36835101 | | [ping.fang@huawei.com](mailto:ping.fang@huawei.com) | |
| Zhiming Ding | | Huawei Technologies Co., Ltd. | | Bldg 7, Vision Software Park, Road Gaoxin Sourth 9, Nanshan District, Shenzhen, Guangdong, China, 518057 | +86 755 36835837 | | [dingzhiming@huawei.com](mailto:dingzhiming@huawei.com) | |
| Phillip Barber | | Huawei Technologies Co., Ltd. | | 1700 Alma Rd, Ste 500  Plano, Texas 75075 USA | +1 972-509-5599 | | [pbarber@huawei.com](mailto:pbarber@huawei.com) | |
| Rob Sun | | Huawei Technologies Co., Ltd. | | Suite 400, 303 Terry Fox Drive, Kanata, Ontario K2K 3J1 | +1 613 2871948 | | Rob.sun@huawei.com | |
| Chengyan Feng | | ZTE Corporation | | No.800, Middle Tianfu Avenue, Hi-tech District, Chengdu, China | +86-28-85342869 | | [feng.chengyan@zte.com.cn](mailto:feng.chengyan@zte.com.cn) | |
| Li Zhu | | ZTE Corporation | | E3048,Bibo Rd,Pudong,shanghai, China | +86-21-68896274 | | zhu.li8@zte.com.cn | |
| Bo Sun | | ZTE Corporation | | J4, ZTE Building, #10 Sth Tangyan Rd., Xi'an, China | +86-29- 88458058 | | [sun.bo1@zte.com.cn](mailto:sun.bo1@zte.com.cn) | |
| Kiseon Ryu | | LG Electronics | | 10225 Willow Creek Rd, San Diego, CA, 92131, USA | +1 (858)-635-5209 | | [kiseon.ryu@lge.com](mailto:kiseon.ryu@lge.com) | |
| Giwon Park | | LG Electronics | | LG R&D Complex 533, Hogye-1dong, Dongan-Gu, Anyang, Kyungki, 431-749, Korea | +82-31-450-1879 | | [giwon.park@lge.com](mailto:giwon.park@lge.com) | |
| Jaehyung Song | | LG Electronics | | LG R&D Complex 533, Hogye-1dong, Dongan-Gu, Anyang, Kyungki, 431-749, Korea | +82-31-450-7898 | | [jaehyung.song@lge.com](mailto:jaehyung.song@lge.com) | |
| Jinsam Kwak | | LG Electronics | | LG R&D Complex 533, Hogye-1dong, Dongan-Gu | +82-31-450-7902 | | [jinsam.kwak@lge.com](mailto:jinsam.kwak@lge.com) | |

# 3. Security Framework

3.1 EAP-RP Support for FILS

### Concept Summary:

* EAP-RP is defined in IETF RFC 5295/5296.
* EAP-RP reduces the number of EAP messages to 1 pair
* Details in 1160/r6 (slides 9, 10, 12)

### Motion:

**Move to add the following statement to the TGai Spec Framework:**

R.3.A: The draft specification shall include support for the EAP-RP [as defined in IETF RFC 5295/5296] for fast authentication by using a pre-established FILS context (EMSK, rRK, rIK) to improve the authentication time during association

**Y:**

**N:**

**A:**

3.2 Optimized EAP Support for FILS

### Concept Summary:

* Reduces the number of messages needed for EAP
* Details in 1160/r6 (slides 13)

### Motion:

**Move to add the following statement to the TGai Spec Framework:**

R.3.B: The draft specification shall include support for the use of optimized EAP by concurrent association, authentication and key distribution to set up initial link and establish the FILS context

**Y:**

**N:**

**A:**

3.3 Concurrent 4-way handshake with Authentication

### Concept Summary:

* Sending of 4-Way Handshake Messages concurrently with EAP/EAP-RP authentication
* Reduces total number of messages
* Details in 1160/r6 (slides 13, 14)

### Motion:

**Move to add the following statement to the TGai Spec Framework:**

R.3.C: The draft specification shall include support for exchanging EAP/EAP-RP messages concurrently to 4-way handshake.

**Y:**

**N:**

**A:**

3.4 Concurrent Authentication & IP address assignment

### Concept Summary:

* Sending of IP address assignment request messages concurrently with EAP/EAP-RP authentication
* Details in 1160/r6 (slides 13, 14)

### Motion 1:

**Move to add the following statement to the TGai Spec Framework:**

R.3.D: The draft specification shall include support for transmitting Authentication, Key-Exchange and High Layer messages (e.g. IP address assignment) concurrently, to improve link setup time

**Y:**

**N:**

**A:**

### Motion 2:

**Move to add the following statement to the TGai Spec Framework:**

The draft specification shall include support for transmitting EAP authentication result to STA without including High Layer messages transmission (e.g. IP address assignment) if authentication finishes before IP address assignment.

Y:

N:

A:

3.5 Encryption of IP Address Assignment Request message

### Concept Summary:

* Include option to allow STA to send IP address assignment request Messages in an un-encrypted manner
  + AP advertises if STA is allowed to send IP address assignment request messahe in an un-encrypted manner
* Allows concurrent backhaul operations
* Details in 1160/r6 (slide 16)

### Motion:

**Move to add the following statement to the TGai Spec Framework:**

R.3.E: The draft specification shall include support for transmitting IP address assignment request message in encrypted and in unencrypted manner by the STA, based on the feature-support indication sent by the AP

**Y:**

**N:**

**A:**