IEEE P802.11
Wireless LANs

|  |
| --- |
| Security related requirements for Specification Frame Work Document  |
| Date: 2012-01-19 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| George Cherian | Qualcomm | 5775 Morehouse Dr., San Diego, CA | 8586516645 | gcherian@qualcomm.com |
| Santosh Abraham | Qualcomm Inc | 5775 Morehouse Dr., San Diego, CA | 8586516107 | sabraham@qualcomm.com |
| Jouni Malinen | Qualcomm Inc | Hermiankatu 6-8 DTampere, Finland |  | jouni@qca.qualcomm.com |

# 3. Security Framework

1. **Include the ability to transmit Authentication, Key-Exchange and High Layer messages (e.g. IP address assignment) in a single frame to improve link setup time**
2. **Include the ability to transmit High Layer messages (e.g. IP address assignment) in encrypted or unencrypted manner**
3. **Include the ability to transmit ANonce in the probe response frame**
4. **Include the ability to transmit ANonce in the beacon frame as an optional feature (assuming ANonce can be changed in every beacon)**
5. **Include the EAP-RP for fast authentication by using a pre-established FILS context (EMSK, rRK, rIK) to improve the authentication time during association (slide 14 of 11/1160r5)**
6. **Include the use of optimized EAP by concurrent 4-way handshake (slide 13 of 11/1160r5) with EAP setup to establish the FILS context**
7. **Include the ability to treat the reception of the MAC layer of ACK of the Association Response that includes the EAPOL element as an Implicit key confirmation and therefore avoid transmission of the Key confirmation message from the STA to the AP**