Group-IKEv2 Usage Instructions

1. **How to upload and run Group-IKEv2:**
    a. Go to directory /Group-IKE/examples/ipsec/g-ike-example
    b. Execute the command: sudo make clean all TARGET=openmote
    c. Upload source code to openmote for GC/KS: sudo make gckserver.upload TARGET=openmote
    d. Upload source code to openmote for member: sudo make member.upload TARGET=openmote
    e. Turn on the motes while having them connected to your machine through USB. You can see the output of each mote by using the command: sudo picocom -b 115200 -r -l /dev/ttyUSB0 --imap lfcrlf
2. **Implementation components:**
    a. **Machine** component declares functions, which are used by all the mealy state machines of IKEv2 and Group-IKEv2. It enables the execution of states and transitions in a mealy state machine.
    b. **Member-machine** contains the states and transitions that a candidate member carries out during Group-IKEv2 handshake.
    c. **GC/KS-machine** includes the states and transitions that GC/KS carries out during Group-IKEv2 handshake.
    d. **G-IKE-Established-machine** declares the functions that are used by both a candidate member and GC/KS once the Group-IKEv2 session is established.
    e. **Common-IKE** component declares functions that are used by all the mealy state machines of both IKEv2 and Group-IKEv2. It enables parsing and creation of particular payloads that both IKEv2 and Group-IKEv2 use.
    f. **G-IKE-Functions** component contains additional functions for Group-IKEv2, which are related to creation and parsing of new payloads and messages.
    g. **Payload** component contains all the payloads dened for IKEv2 and Group IKEv2 protocols.
    h. **Auth** component contains functions related to the authentication mechanism used in IKE AUTH and GSA AUTH messages.
    i. **PRF** component denes pseudo-random functions which are used by Auth component during authentication.
    j. **ECDH** component includes functions related to signature generation for Certificates.
3. **How to change settings in Group-IKEv2 implementation:**
    a. In order to change settings such as encryption, integrity, authentication method you have to change the settings defined in the project conf file, g-ike-example-conf.h file.
    b. In order to add more members in the group you have to add the new members in g-ike-conf.h file and in the table member_param_t gpad_table in spd-conf.c file.

For additional information regarding this implementation you can also refer to the file “Insturctions.pdf” in openmote-ike folder.