|  |
| --- |
| MN Initiated Join/Leave operation explanation in D002 |
| Date: 2013-05-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | Email |
| Antonio de la Oliva | University Carlos III of Madrid |  |  | aoliva@it.uc3m.es |
| Albert Banchs | Institute IMDEA Networks |  |  | **albert.banchs@imdea.org** |

* + 1. Secure group manipulation with group key distribution

Figure 45 illustrates group manipulation command distribution initiated by a Command Center via a multicast channel. The MIH User of the Command Center generates a MIH\_Net\_Group\_Manipulate.request, described in 7.4.32, and then it passes the request to the MIHF of the Command Center. Upon receiving the request, the MIHF generates MIH\_Net\_Group\_Manipulate indication (Note that the decision on sending an indication message or a request message depends on the ResponseFlag parameter of the MIH\_Net\_Group\_Manipulate.request primitive), described in 8.6.1.24, and sends it to MNs via multicast ~~channels~~ transport. When an MN receives the MIH\_Net\_Group\_Manipulate indication message, the MIHF of the MN processes the message. After processing the message, the MIHF sends MIH\_Group\_Manipulate.indication to the MIH User of the MN.



1. —Example of group manipulation distribution using multicast mechanisms

In a typical example, an MIH User of a Command Center generates MIH\_Net\_Group\_Manipulate.request described in 7.4.32 as follows:

1. Define a group to manipulate. If it is a new group, choose a GroupIdentifer which is not currently in use by consulting with the Group Management Database. Then, decide group members, i.e. MNs, of the group and a group key for the group. For an already existing group, new members to be added to the group are added to the group members, and members to be removed from the group are removed from the group members.
2. Send to the GKB Generator all the Device Keys, the Leaf Numbers of the group members determined in a) and the group key. Then, the MIH User receives from the GKB generator a GKB or a set of GKBs: A GKB contains a CompleteSubtree field, a GroupKeyData field and optionally a SubgroupRange field. A SubgroupRange is a pair of Leaf Numbers and defines a range of Leaf Numbers. A simple example which shows how to make those fields is given in Annex P. A GKB contains a SubgroupRange field if it is one of divided GKBs. Note that one MIH\_Net\_Group\_Manipulate.request contains one and only one GKB. Plural GKBs result in plural requests.
3. (Optional.) Define the AuxData field.
4. Define a DestinationIdentifier. A DestinationIdentifier is a Group MIHF ID which represents an existing group. Care is required to distribute a divided GKB. The SubgroupRange indicates the MNs which are the distribution targets of the GKB. If an MN is in the range, it should receive the divided GKB.
5. Generate an MIH\_Net\_Group\_Manipulate.request from the DestinationIdentifier, the GroupIdentifier, the SubgroupRange (an option), the VerifyGroupKey (an option), the AuxData (an option), the CompleteSubtree and the GroupKeyData (an option). Set the GroupKeyUpdateFlag if the group key of the group designated by the GroupIdentifier should be updated. Send it to the local MIHF.
6. Update the Group Management Database. If the target group of manipulation is an existing group, add/remove members (MIHF IDs, Device Keys and Leaf Numbers) and update its group key. If the target group is a new one, add a new Group MIHF ID (= GroupIdentifier) with its new members and its new group key.

When the MIHF of the Command Center receives an MIH\_Net\_Group\_Manipulate.request which is generated by the MIH User, the MIHF generates and sends an MIH\_Net\_Group\_Manipulate indication message to a multicast ~~channel~~ transport.

1. Generate a Source MIHF ID TLV using its own individual MIHF ID.
2. Generate a Destination MIHF ID TLV from the DestinationIdentifiner in the received MIH\_Group\_Manipulate.request.
3. Generate a Group Identifier TLV from the GroupIdentifier in the received MIH\_Group\_Manipulation.request.
4. Generate, as needed, a Multicast Address TLV from the multicast address corresponding to the GroupIdentifier in the received MIH\_Net\_Group\_Manipulate.request. The Multicast Address Database serves for the purpose of finding the multicast address.
5. (Optional) Generate a SubgroupRange TLV from the SubgroupRange in the received MIH\_Net\_Group\_Manipulate.request.
6. (Optional) Generate a Verify Group Key TLV from the VerifyGroupKey in the received MIH\_Net\_Group\_Manipulate.request.
7. (Optional) Generate an Aux Data TLV from the AuxData in the received MIH\_Net\_Group\_Manipulate.request.
8. Generate a Complete Subtree TLV from the CompleteSubtree in the received MIH\_Net\_Group\_Manipulate.request.
9. Generate a Group Key Data TLV from the GroupKeyData in the received MIH\_Net\_Group\_Manipulate.request.
10. Generate a Signature TLV shown in 8.4.2 using the signing key of the Command Center.
11. Generate an MIH\_Net\_Group\_Manipulate indication using the preceding TLVs. If necessary, its Service Specific TLVs are so encrypted that they make a Security TLV.
12. Send the MIH\_Net\_Group\_Manipulate indication message created in k) to the multicast address corresponding to the DestinationIdentifier.
13. Update the Multicast Address Database if necessary. It is assumed that the MIHF is equipped with a mean to obtain a multicast address associated with a Group MIHF ID. The multicast address may be contained in the MIH\_Net\_Group\_Manipulate.request received from the MIH User. If the DestinationIdentifier in the received request is not registered in the database, obtain the multicast address associated with the DestinationIdentifier and update the database with the DestinationIdentifier and the associated multicast address.

When a client MN receives a group manipulation command, i.e., an MIH\_Net\_Group\_Manipulate indication message, issued by a Command Center, the MIHF of the MN processes the command. Suppose at first that the GKB in the group manipulation command has a group key data part:

1. The MIHF obtains a Source Identifier from the Source MIHF ID TLV.
2. The MIHF verifies the Signature TLV using the verification key corresponding to the obtained SourceIdentifier. If the verification fails, the MIHF shall cancel the following steps and stop processing the command.
3. The MIHF checks the DestinationIdentifier in the Destination MIHF ID TLV. If the DestinationIdentifier does not match one of the following MIHF IDs, the MIHF shall cancel the following steps and stop processing the command: (i) A Group MIHF ID corresponding to a broadcast address, (ii) a Group MIHF ID which is registered with a multicast address in the Group Database, or (iii) the MN's own individual MIHF ID.
4. Decrypt the payload if it is encrypted, i.e., if it is a Security TLV. The decryption key is the one associated with the DesitinationIdentifier in the Group Database.
5. If a SubgroupRange TLV exists in the indication, the MIHF obtains a SubgroupRange and check whether its own Leaf Number is contained in the SubgroupRange or not. If it is not, the MIHF shall cancel the following steps and stop processing.
6. The MIHF obtains the GroupIdentifier in the Group Identifier TLV.
7. A GKB is comprised of the Complete Subtree TLV, the Group Key Data TLV and optionally the Verify Group Key TLV. The MIHF processes the Complete Subtree TLV and the Group Key Data TLV as described in 9.4.2.2.2. If a Verify Group Key TLV exists, the MIHF verifies the group key derived from the GKB. If a group key is obtained (and verified), go to the next step. Otherwise, go to Step i).
	1. In case an MN cannot decrypt the Security TLV, the message will be silently discarded.
8. The MIHF checks whether the GroupIdentifier obtained in Step f) has already been registered or not in the Group Database. If it has been, go to Step j) [Stay]. Otherwise, go to Step k) [Join].
9. The MIHF checks whether the GroupIdentifier has already been registered or not in the Group Database. If it has been, go to Step m) [Leave]. Otherwise, go to Step j) [Stay].
10. [Stay] The MIHF throws an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field of the indication shall be “Unchanged successful” (5). The procedure of command processing terminates.
11. [Join] The MIHF obtains a multicast address associated with the GroupIdentifier and starts listening to it. The messages come through the multicast channel may be encrypted with the group key obtained in Step g). The multicast address may be obtained from a server. Or, the received indication may accompany it in the Multicast Address TLV. Save in the Group Database the GroupIdentifier, the associated multicast address and the group key obtained in Step f).
12. The MIHF throws an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field must be “Join operation successful” (0). The procedure of command processing terminates.
13. [Leave] The MIHF finds the multicast address recorded on the same row as the GroupIdentifier obtained in Step f) and the MIHF stops listening to it. The MIHF discards the row which has the GroupIdentifier.
14. The MIHF throws an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field must be “Leave operation successful” (3). The procedure of command processing terminates.

Then, suppose that the GKB in the group manipulation command has no group key data part:

1. The MIHF obtains a Source Identifier from the Source MIHF ID TLV.
2. The MIHF verifies the Signature TLV using the verification key corresponding to the obtained SourceIdentifier. If the verification fails, the MIHF shall cancel the following steps and stop processing the command.
3. The MIHF checks the DestinationIdentifier in the Destination MIHF ID TLV. If the DestinationIdentifier does not match one of the following MIHF IDs, the MIHF shall cancel the following steps and stop processing the command: (i) A Group MIHF ID corresponding to a broadcast address, (ii) a Group MIHF ID which is registered with a multicast address in the Group Database, or (iii) the MN's own individual MIHF ID.
4. Decrypt the payload if it is encrypted, i.e., if it is a Security TLV. The decryption key is the one associated with the DesitinationIdentifier in the Group Database.
5. If a SubgroupRange TLV exists in the indication, the MIHF obtains a SubgroupRange and check whether its own Leaf Number is contained in the SubgroupRange or not. If it is not, the MIHF shall cancel the following steps and stop processing.
6. The MIHF obtains a GroupIdentifier in the Group Identifier TLV.
7. A GKB is comprised of the Complete Subtree TLV. The MIHF processes the Complete Subtree TLV as described in 9.4.2.2.2. If the MIHF succeeds to find a matching pair of GKB Indices, go to the next step. Otherwise, go to Step i).
8. The MIHF checks whether the GroupIdentifier obtained in Step f) has already been registered or not in the Group Database. If it has been, go to the Step j) [Stay]. Otherwise, go to Step k) [Join].
9. The MIHF checks whether the GroupIdentifier obtained in Step f) has already been registered or not in the Group Database. If it has been, go to Step m) [Leave]. Otherwise, go to Step j) [Stay].
10. [Stay] The MIHF throws an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field of the indication must be “Unchanged successful” (5). The process terminates.
11. [Join] The MIHF obtains a multicast address associated with the GroupIdentifier and starts listening to it. The multicast address may be obtained from a server. Or, the received indication may accompany it in the Multicast Address TLV. Save in the Group Database the GroupIdentifier, the associated multicast address.
12. The MIHF throws an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field must be “Join operation successful” (0). The procedure of command processing terminates.
13. [Leave] The MIHF finds the multicast address recorded on the same row as the GroupIdentifier obtained in f) and the MIHF stops listening to it. The MIHF discards the row which has the GroupIdentifier.
14. The MIHF throws an MIH\_Net\_Group\_Manipulate.indication described in 7.4.32.2 to the MIH User. The GroupStatus field must be “Leave operation successful” (3). The procedure of command processing terminates.

Section 7.4.31 introduces a mechanism enabling the MN to trigger the Join/Leave operations controlled by the Command Center. In order to do so, the MIH User located at the MN notifies the Command Center of its desire to Join or Leave a group through the use of the MIH\_MN\_Group\_Manipulate primitive. The Command Center, upon receiving the associated request message, performs the same process as defined in this section, for the use of the MIH\_Net\_Group\_Manipulate although in this case, the group to be manipulated is provided by the MN. The resulting GKB parameters are returned to the MN in the MIH\_MN\_Group\_Manipulate response message.