IEEE P802.21
Media Independent Handover Services

|  |
| --- |
| How an MN determines whether it belongs to a group? |
| Date: 2013-11-xx |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Lily Chen | NIST | 100 Bureau Dr. Gaithersburg, MD 20878 | +1 (301) 975-6974 | Lily.Chen at nist.gov |

Abstract

This contribution discuss an issue presented in the IEEE P802.21d/D2.0 with regard to how an MN determines it belongs to or does not belong to a group to resolve comment #87.

In the current IEEE 802.21d, the following text and subclause 9.4.2.5.1 indicate that an MN can determine that it does not belong to the group in two situations.

1. The MN cannot find a matching GKB index; or

2. The MN can find a matching GKB index but fail to recover the MGK.

If an MN belongs to the group, then it must be able to successfully recover MGK. That is, an MN cannot be assured belonging to the group until it recovers an MGK (and verifies it by “GroupKeyVerificationCode”). [That is, GroupKeyVerificationCode cannot be optional.]

If an MN does not belong to the group, it can find out either by failing to find the matched index or by failing to recover the MGK, which means even a matching index is included for an MN, it may not belong to the group. This can be problematic.

Is the group manipulation command the only way to inform an MN to join or leave?

**9.4.1 MIH message protection mechanisms using GKB-generated SAs**

Group Key Block (GKB) is a data field used to distribute master group keys (MGKs) to protect MIH multicast/broadcast commands. A GKB contains GroupKeyVerificationCode, CompleteSubtree and GroupKeyData (see 7.4.31.3 and 7.4.32.1). A group manipulation command accompanies a target MIHF Group ID and a GKB. An MN follows the procedure described in 9.4.2.5.2 to determine whether it should try to recover the key from the GKB. If an MN succeeds in recovering am MGK, the MN will keep the pair of the target MIHF Group ID and the MGK, which means that the MN belongs to the group designated by the target MIHF Group ID. Otherwise, if an MN fails to derive an MGK from the GKB, it means that the MN does not belong to the group designated by the target MIHF Group ID. Then, the MN leaves the group discarding the stored pair of MIHF Group ID and MGK.

**9.4.2.5.2 Decapsulation**

At first, the decapsulation procedure for a GKB with a group key data part is described as follows:

1. An MIHF finds a GKB Index in the complete subtree part of the GKB and a Device Key Unit in the Device Key that the MIHF itself owns such that the GKB Index and the GKB Index of the Device Key Unit are identical. Suppose that the GKB Index thus found is the n-th GKB Index in the complete subtree part. If the MIHF fails to find such GKB Indices, the procedure shall terminate.
* If the procedure terminates here, it means that the MN does not belong to the group designated by the TargetIdentifier defined in 7.4.32.1. The MN shall leave the group if it currently belongs to the group.
1. Using the Node Key in the Device Key Unit found in a), the MIHF decrypts the n-th encrypted group key in the group key data part. The result of the decryption is a group key KG.
* The group key KG is the group key for the group designated by the TargetIdentifier. The MN shall belong to the group.
1. If there exists a field of VerifyGroupCode in the MIH\_Net\_Group\_Manipulate.request defined in 7.4.32.1, check the MAC in the VerifyGroupCode field using the group key KG. If it fails, the decapsulation procedure shall abort.

Conclusion:

1. It must be clarified how an MN determines whether belonging to a specific group. It is more reasonable to use the GKB index to indicate to an MN whether it belongs to the group.
2. “GroupKeyVerificationCode” cannot be optional, when KeyData field is not empty.