# MSI comments on ETG 17-065 Group Key Management.docx

| **#[[1]](#footnote-1)** | **Page** | **Section** | **Imp.[[2]](#footnote-2)** | **Status** | **Comment/Recommendation** | **Resolution** |
| --- | --- | --- | --- | --- | --- | --- |
| MS1 | 1 | Title | E | R | Referring to the first comment in the margin, current title is ok as shown. | Cool. Will remove comment from word doc in next revision.  |
| MS2 | 1 | Par 1 | T | R | Discuss requiring a minimum number of groups per SU and what a minimum requirement value should be.MSI believes use of groups may not be necessary for CFNS channels is optional for customers and so, optional for manufacturers. We also don’t see the need for an SU to be in more than 1 group per LLE domain.Open to discussion.  | Harris believes that efficient key replacement after a key compromise may require hierarchical groups. Not clear to us how one key helps at all(?).Discuss.Discussion: MSI agrees that there are efficiency gains from having more than one key, and that interop requires that a minimum number be specified.We agree the number is greater than 1, and will hope to come to some decision in Mesa based on actual math.FBI says that without specifying that groups rekeying is required, then operations are compromised for organizations that buy radios from multiple vendors.  |
| MS3 | 1 | Par 2 | T | R | This suggests an SU that receives keys (via individual or group method) for a group that it was not previously a member of should assume it is a member of that group. This introduces the scenario of modifying an SUs group membership after the SU has exchanged inventory summary information with the domain’s LEF(i.e. SU is active in the LLE domain) and have likely had their group membership and group key inventories synched with the LEF. While the method for creating membership in a new group seems feasible, what about group membership changes that remove an SU from a group? Suggest a procedure in which an SU learns it is no longer a member of a group, then it shall delete the keys for that group. Open to discussion. | Maybe we need to explain it in the text, but that procedure would be a that the LEF would request an inventory summary. The LGID digest wouldn’t match, so there would be a detailed LGID inventory and the SU would remove itself from the group and delete keys. Discuss.Agreed Resolution: No change required. |
| MS4 | 1 | Par 6 | T | O | Key management following a key rotation needs to be discussed. After a rotation, should SUs active in the domain be able to request new future keys?If so, how is request flooding prevented? | Discuss. Are you talking about group keys or operational keys. For operational keys, that’s addressed elsewhere in the document.For group keys, the LEF controls it all. Here, the LEF would send out a new group key secured by the previous group key. At some point, the SU is either going to see that key, or, if he registers, he’ll fail his inventory and get updated.[TOM WILL CHECK TO SEE WHAT WE’VE AGREED REGARDING OPERATIONAL KEYS AND WHETHER IT COMPLICATES GROUP KEYS] |
| MS5 | 1 | Par 4 | E | R | The paragraph describes that a trunked radio will send the Inventory Summary after completing Unit Registration, or optionally upon query from the RFSS. Suggest a clarification that the radio will send the Inventory Summary at the earliest opportune time after completing registration and affiliation in trunking.How does the radio know whether it must send the Inventory Summary after the Registration, or wait for a query from the RFSS? | “opportune” – sure.When to send summary….Discuss.Added “at the earliest opportune time” means the radio gets to decide. Hopefully this fits in the unit registration itself. |
| MS6 | 1 | Par 4 | E | R | The Inventory Summary may not necessarily be sent to the LEF. It could be sent to another network element that knows the hashed digest of the SU’s group keys. That network element would contact the LEF if the summary does not match the hashed digest. Should the first sentence be changed to: "When a trunking SU completes its full registration within a domain, it sends an Inventory Summary (1) to the RFSS, in order to help the LEF determine whether it needs to send any group keys to the SU"?  | Since we use the LEF to refer to whatever part of the FNE does LLE key management, I think it’s fine the way it is.Discuss.Agreed: We’re talking about a function, not a device. |
|  |  |  |  |  |  |  |

1. Company initials (up to 2) and a sequential number to identify the comment. [↑](#footnote-ref-1)
2. IMP: Importance. E = Editorial – Fix it if you agree. T- = Minor Technical – Fix it if you agree. T = Significant Technical – Discuss it if you don’t agree, T+ = Major Technical – could result in a negative ballot if not resolved. [↑](#footnote-ref-2)