## Management of Group Membership and Keys

Section 4.6.4

Note: This contains some on-gong discussion (in the comments) between Andy Davis of MSI and Tom Hengeveld of Harris. These will be suitably decanted into a comment matrix when we review the document.

The membership and organization of groups within a domain is up to the LEF of the domain. For interoperability purposes, SU should support some standard minimum of number of groups, and a current and future key for each group. Group Key Management consists of a series of opportunistic exchanges between SU and the LEF of a domain.

Editor’s Note: FBI representative to ETG say that without specifying that group rekeying is required, then operations are compromised for organizations that buy radios from multiple vendors.

Group keys may be distributed using individual or group methods. An LEF determines which methods to use based on its understanding of the group key inventories of the SU’s under its control, and of which SU may be present in the domain. When an SU receives a group key (either individually or by group methods) for a group that it is not currently a member of, it implicitly becomes a member of the group.

The high-level flow of Group Key Management is illustrated in Figure 1[[1]](#footnote-1) and relies on the inventory summary of Figure 2. The inventory summary contains the number of LLE groups of which the SU is a member, an SHA-256 digest of the LGIDs of those groups, and an SHA-256 digest of the current and future GKIDs of its groups. By comparing the summary provided by the SU to that computed from the ‘desired state’ of the SU, the FNE can determine whether the SU’s group membership is correct, and whether its group key inventory is correct.

When a trunking SU completes its full registration within a domain, it sends an Inventory Summary (1), at the earliest opportune time, to the LEF to help the LEF determine whether it needs to send any group keys to the SU. (Alternatively, an LEF can request an Inventory Summary from an SU at any time (5).) Likewise, conventional SU operating in a CFN domain should send an inventory summary to the LEF at a convenient time upon entering a CFN domain. Based on the inventory summary, the LEF can determine which detailed inventory information (if any) is required to determine how to bring the SUs keys up to date. If the LGID inventory doesn’t match, the LEF requests more a detailed inventory information group membership (2a,b) and corrects the LGID membership list of the SU (2c), and provides the keys for any missing groups (2d). Subsequently, the LEF should request a new inventory summary.

If only the key summary is incorrect, the FNE requests a detailed key inventory (3a,b), and subsequently uses individual or group methods (4) to provide or remove the mismatched keys.

LEF opportunistically send OSPs to announce the current and future group key ids for LLE group. SU that are members of the group and lack one or more keys can request the given key or keys from the LEF. The LEF then uses suitable individual or group methods to provide the keys, if appropriate.

All group key messaging is LLE encrypted.



Figure , High Level Flow for Group Key Inventory and Management



Figure 2, Inventory Summary

1. For simplicity, routine acknowledgements are not illustrated in the figure. [↑](#footnote-ref-1)