

| Abbreviations |
|---|
| ~M = macAP_3 |
| ~M_1 = macUE_3 |
| ~M_2 = enc((NMK_2,groupKey),KEK_3,1) |
| ~M_3 = HASH_MAC256((ADDID(macAP_3,macUE_3),1,enc((NMK_2,groupKey),KEK_3,1)),MAK_3) |
| ~M_4 = macAP_3 |
| ~M_5 = macUE_3 |
| ~M_6 = enc((NMK_3,groupKey),KEK_3,1) |
| ~M_7 = HASH_MAC256((ADDID(macAP_3,macUE_3),1,enc((NMK_3,groupKey),KEK_3,1)),MAK_3) |
| ~M_8 = macAP_3 |
| ~M_9 = macUE_3 |
| ~M_10 = enc((NMK_4,groupKey),KEK_3,1) |
| ~M_11 = HASH_MAC256((ADDID(macAP_3,macUE_3),1,enc((NMK_4,groupKey),KEK_3,1)),MAK_3) |

A trace has been found.

