\*\*\*\* Deleted all old comments from this version \*\*\*\*

| **#[[1]](#footnote-1)** | **Page** | **Section** | **Paragraph, Figure, Table** | **IMP**[[2]](#footnote-2) | **Status[[3]](#footnote-3)** | **Comment / Recommendation****(e.g. what needs to be fixed and why)** | **Summary of Discussion / Resolution** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| MS090 | 54 | 4.1.2.7 |  | T | R | Zeroization needs further discussion and separate consideration for Trunking and Conventional. See comments on section 4.7. | Ok, do you want to discuss it now or then?<COME BACK TO THIS AFTER 4.7>Resolution: In R10 or so we replaced 4.1.2.7 with a change to the IKSP that includes the domain. 4.1.2.7 was deleted.AD: Comment is not longer relevant. OK to close. |
| MS094 | 54 | 4.1.4.1 |  | T | R | Zeroization needs further discussion and separate consideration for Trunking and Conventional. How are Home vs Foreign Domains determined or tagged?There seems to be no reason code for an LEF deleting the keys in its domain only. What are the use cases for an LEF to zeroize the LLE keys of another LEFs domains. | 1) Domains are identified by their domain ids. Section 4.7 describes this.2) Specific foreign domain.3) The home LEF should be able to deauthorize a unit to operate in other domains.Proposed Resolution: No change.<COME BACK TO THIS AFTER 4.7>Resolution: In R10, we deleted everything in 4.1.4.1 except the ability to optionally zeroize the ILEK and any stored IKSPs. No further change required.AD: Comment is no longer relevant. OK to close.  |
| MS095 | 56 | 4.1.4.1 | Table 11 | T | R | Should there be an option to Zeroize Home Domain? | I don’t believe so. It doesn’t make sense to me to zeroize the home domain without zeroizing all domains.Proposed Resolution: No change.<COME BACK TO THIS AFTER 4.7>See MS094. We deleted this section.No further change required.AD: Comment is no longer relevant. OK to close. |
| MS122 | 70 | 4.5.2 |  |  | R | Zeroization needs further discussion and separate consideration for Trunking and Conventional. See comments on section 4.7. | Proposed Resolution: Included in 4.2.2.6.AD: Comment is no longer relevant. OK to close. |
| MS136 | 81 | 4.6.4 |  | T | R |  This section needs to discuss how indication of active/future GLEK by group is provided and how an SU may indicate the need for either.  |  Discuss.How group key inventory/distribution is done is still an open issue that needs to balance air interface efficiency vs robustness and LEF complexity. Section 4.6.4 is being reviewed under separate cover and will be reincorporated into the overview when complete. |
| MS138 | 83 | 4.7.2 |  | T | R | Presumably the degree of zeroization permitted is determined by whether the zeroization message is protected with an IMAK (derived from IKSP so message sourced by foreign LEF) or an H-IMAK (derived from ILEK so message sourced by home LEF), true? Note that in conventional, every LLE domain is considered a home domain. | Discuss this nearly identical but more tactfully put comment along with MS137. Yes, the key SU knows that the LEF is authorized to do the operation based on which IMAK it uses.Resolution: The IKSP now includes the domain that the SU is operating in. So this comment is obsolete. No further change required.AD: Comment is no longer relevant. OK to close. |
| MS140 | 83 | 4.7.3 | Bullet 1 | T | R | How does the SU know whether to use the IKSP or the ILEK to generate the MAK and authenticate the message? | Within its home domain, it uses the H-IMAK. Outside of it, it uses the IKSP.Resolution: See MS138. It uses the IKSP for the domain in which it is operating. No further change required.AD: Comment is no longer relevant. OK to close. |
| MS141 | 83 | 4.7.3 | Bullet 1 | T | R | Why isn’t the Zeroization command protected with an IKEK? | Does it need to be encrypted? It’s already link layer encrypted and it’s not a key, so it doesn’t need to be protected that way.Proposed Resolution: No change.AD: Discuss zeroization OSP target; group vs. individual and respective protection and authentication.Harris believes no further changes are required. Discuss.In Section 4.7.2: “Zeroization messages are authenticated using the IMAK of the SU that is applicable to the current domain.” Harris believes this clarifies the text and that no further revisions are required. |
| MS142 | 83 | 4.7.3 | Bullet 2 | T | R | If the Zeroization Command Body indicates specific domains to be zeroized, what is the purpose of the commands listed in section 4.1.4.1? | Brevity. Only it provides a shorthand for the most commonly used (I think) functions.Proposed Resolution: No change.Domains in the message were was removed in R10. No further change required.AD: Comment is no longer relevant. OK to close. |
| MS143 | 84 |  | Figure 41 | T | R | Should IKEK be IKSP? | Not the way it’s drawn. Made an editorial change in R12 to clarify.In R14, Page 90, Figure 40. There used to be separate figures for home/foreign domains. 41 was for the foreign domain (See the original PDF).In Section 4.7.2: “Zeroization messages are authenticated using the IMAK of the SU that is applicable to the current domain.” Harris believes this clarifies the text and that no further revisions are required. |
| H201 |  | 4.4.5 | Fig 33 and Text | E | R | Figure refers to GKID/GKSN. Needs to be updated for LGID/GKID. | Done in R14. |
| H202 |  | 4.5.3 | Fig 37 | E | R | Figure refers to GKID/GKSN. Needs to be updated for LGID/GKID. | Done in R14 |
| H203 |  | 4.6.3 | Fig 39 | E | R | Figure refers to GKID/GKSN. Needs to be updated for LGID/GKID (Delivered and Security Key) | Done in R14. |

1. Axx = Airbus, Cxx = Codan, Exx = Etherstack, Hxx = Harris, Ixx = ICOM, Jxx = EF Johnson, Mxx = Motorola, Rxx = Relm, Txx = Tait, etc. xx = Comment Number [↑](#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)
3. Status = Open (further discussion required), PR = Proposed Resolution, AR = Agreed Resolution, Closed (document updated with AR) [↑](#footnote-ref-3)