

---

**Title:** **DRAFT** Response LS (to R2-041261) on Re-authentication and key set change during inter-system handover  
**Response to:** R2-041261 = S3-040462  
**Release:** Release 5  
**Work Item:** --  
  
**Source:** SA3  
**To:** RAN2  
**Cc:** CN1, RAN3

**Contact Person:**

**Name:** Marc Blommaert, Siemens  
**Tel. Number:** +32 14 25 3411  
**E-mail Address:** [Marc.Blommaert@Siemens.com](mailto:Marc.Blommaert@Siemens.com)

---

**1. Overall Description:**

SA3 thanks GERAN2 for the questions posed in the LS R2-041261.

Question-1: *“Is it the understanding that the specifications permit that the AKA procedure providing new keys to the UE may be performed significantly in advance of the corresponding Security/Ciphering Control procedures that activate these new keys? If so, in what proportion of cases does this currently occur?”*

Answer: SA3 is the opinion that new keys should be taken into use as soon as possible, as there seems to be no reason to delay the activation of new keys. SA3 have noted that there exists no clause within TS 33.102 specifying this exactly, but as the TS 33.102 is not in contradiction with this, SA3 sees currently no need for changing TS 33.102.

Question-2: *“Are the new keys that are not activated considered as new keys in the next signalling connection? (i.e. “Key Status” to RNC is indicated as ‘new’ in the security mode command.)”*

Answer: SA3 think that the -not activated- keys can be considered as new.

Question-3: *“Could SA3 clarify what the intention of their specification is, especially with respect to the scenario described above?”*

*“If new keys are received during a RRC connection but they are not activated during a signalling connection and a second security mode command is received for a following signalling connection to the same domain (and same RRC connection) are those keys to be activated or not with the second security mode command?”*

Answer: Also for the above described scenario the key can be considered as new, and hence should be activated with the second security mode command.

**2. Actions:**

To RAN2 group.

**ACTION:** SA3 asks RAN2 to reply if they see a need to change the SA3 specification.

**3. Date of Next TSG SA WG 3 Meetings:**

TSG-SA3 Meeting #35 5-8 October 2004 Malta

TSG-SA3 Meeting #36 23-26 November 2004 Shenzhen, China