**3GPP TSG SA WG3 Security — S3#18** **S3-010154**

**21 - 24 May, 2001**

**Phoenix, USA**

---

## TSG-RAN Working Group 2 (Radio L2 and Radio L3) *R2-010982*
## Hayama, Japan, 9 - 13 April 2001

**Source: TSG-RAN WG2**

**To: TSG-SA WG3**

**Cc:**

**Title: LS on Wrap around of the calculated START value**

**Contact:** Ainkaran Krishnarajah, Ericsson
Email: Ainkaran.Krishnarajah@era.ericsson.se

---

TSG RAN WG2 has indentified the need to handle the wrap around of the START value as calculated in TS 25.331 v3.6.0, in Section 8.5.9. TSG RAN WG2 understands that this situation is rare, as it is likely that there will be at least one authentication procedure for an RRC connection that exists for a sufficiently long time. However, it is possible that the START calculation may yield a value that is the maximum (the 20 MSBs are all 1s for the highest COUNT-C/I in a CN domain, for all radio bearers and signalling radio bearers) for connections that exist for a very long time and/or for high data rate connections. Consider for example, a TM RLC radio bearer in which the Connection Frame Number (CFN) is used as the LSBs of the COUNT-C. The CFN increments the COUNT-C for TM RLC every 10ms.
It is undefined how the wrap around of START should be handled. Two options exits:

1) The START value for the respective CN domain is kept at the maximum value
2) The START value for the respective CN domain is set to zero when it is wrapped around.

TSG RAN WG2 considers Option 1 as an undesirable choice as this would mean that a radio bearer could potentially use the same inputs to the ciphering algorithm for a particular radio bearer.
TSG RAN WG2 would consider that Option 2 is the best choice (this will not affect the existing radio bearers and/or signalling radio bearers) and would like to ask TSG SA WG3 to confirm if this solution is acceptable from a security point of view.
TSG RAN WG2 would also welcome any proposals from TSG SA WG3 on how to handle START at the maximum value.
TSG RAN WG2 also sees that updates are required in TS 33.102 to capture the preferred solution.