TSG-SA WG3 (Security) meeting #12
Stockholm, Sweden, 11-14 April 2000

S3-000243

Agenda Item: 12.2

Source: Ericsson

Title: Cipher and Integrity key update

Document for: Discussion

Current version of 3GPP TS 33.102 v3.4.0, includes a new requirement for VLR/SGSN on key lifetime supervision and update:

Chapter 6.5.4.2, “IK”:

“…The MSC/VLR or SGSN shall assure that the IK is updated at least once every 24 hours. …”

Chapter 6.6.4.2, “CK”:

“…The MSC/VLR or SGSN shall assure that the CK is updated at least once every 24 hours. …”

This new requirement on VLR/SGSN introduces further implications that have not been considered:

- Definition and handling of new timers,
- Impacts on the transfer of authentication data within same SN domain,
- Will keys be updated even if MS is in idle mode most of the time? …

Besides, some other mechanisms to control the lifetime of the cipher and integrity keys are already specified in TS 33.102 (see chapter 6.4.3. on “Cipher key and integrity key lifetime”). The mechanisms described there reside at the USIM instead, providing the HE control of key lifetime supervision and update.

The rest of S3 members are kindly requested to provide clarifications on the nature and applicability (R99 or R00) of this new requirement.

It is also suggested that the indication that *“the VLR/SGSN shall assure that IK and CK are updated at least once every 24 hours”* is removed from TS 33.102 at least until all the implications identified by this contribution are clarified.