3GPP TSG SA WG3 Security — S3#17 **S3z010015**

27 February - 02 March, 2001

Gothenburg, Sweden

Title: **LS on LCS message security**

Source: **TSG SA WG3**
To: **TSG GERAN**
Cc:
Contact Person: **Greg Rose, ggr@qualcomm.com**

A draft version of this LS was unintentionally distributed in the GERAN LCS ad hoc - meeting before this final LS was agreed in S3. Since there are differences between this final version and the draft version please study this LS extremely carefully.

A number of contributions were presented to S3#17 in Gothenburg, Sweden, regarding various options for ciphering and security for Location Services (LCS) messages between the SMLC and the MS. These included documents S3-010008 (from GERAN), S3-010069 (from Nokia) and S3-010088 (from Ericsson). Since LCS discussions were underway at the same time as the S3 meeting, we understood some of the options mentioned in these contributions to have been ruled out already.

This liaison comments only on issues of security of messages between the SMLC and the MS. At issue is the fact that the SMLC actually resides at the base station subsystem. S3 notes that if the SMLC was located somewhere else in the serving network, the messages would normally be sent to the SGSN, encrypted there, and sent onward to the MS.

S3-010069 describes two architectures:

- **LLC split** in which the messages are cryptographically protected at the SMLC and transmitted directly to the MS without going through the SGSN
- **SGSN routing** in which the messages are transmitted between the MS and the SMLC via the SGSN where they are cryptographically protected.

While the LLC split architecture appears simpler and more efficient in terms of network traffic for the LCS messages, there are some concerns about security relating to key management that are not addressed in S3-010069. To cryptographically protect the messages, a ciphering key must be provided to the SMLC (or BSS). There are two cases to examine:

- **If the current Kc key is provided to the SMLC:** it is absolutely essential that this key be well protected. It must be transmitted to the SMLC securely, relying heavily on Network Domain Security for that protection. Furthermore, since this key controls all information flowing to or from the MS, it is very sensitive (much more than the LCS information itself) and must be protected at the SMLC. S3 strongly recommends not using this alternative.
- **If a new key is provided to the SMLC**: this key must be calculated from the Kc key using a one-way function, which is not yet defined. Support for this function must also be included in the MS, which does not currently require any such functionality. Since the key protects only LCS messages, it has the same sensitivity as the LCS messages themselves, and does not require further protection. (It is assumed that Network Domain Security would be applied to these messages in

either approach, but at the moment such messages are not protected within the network.) At the LLC layer, the MS must be able to recognise which messages are LCS messages encrypted with a different key, while the BSS must be able to recognise these messages and route them to the SMLC; this complication might have unforeseen security implications.

S3 considers “LLC Split with current Kc” too difficult to make secure. Both of the other alternatives, “LLC Split with derived key” and “SGSN Routing” rely to some extent on Network Domain Security to protect messages from the SMLC to the SGSN. Again it must be noted that there is currently no such security applied. There are no security reasons to prefer either approach, although the more complicated key management required for the “LLC split with new keys” approach would require detailed study and development and deployment of new key generation algorithms in the MS and the network.