Source:	**TSG SA WG3**
To:	**TSG SA WG1, TSG SA WG2**
Title:	**Reply LS on "Enhanced user privacy for location services "**
Contact:	**Stefan Schröder**
Email:	**stefan.schroeder@t-mobile.de**

Overall Description:

This LS is a reply to WG2's LS S2-013063 (S3-010575). S3 thanks SA2 for being asked and is pleased to provide the following feedback. Updated document versions [1] and [2] were taken into account.

Feedback:

SA3 welcomes the suggested enhancements to user privacy for LCS regarding an *authorization* based on

- LCS Client

- Service Identity

- Requestor Identity

LCS is a delicate issue both in user's and national regulators' view, so there is a strict need to also *authenticate* all parties involved. SA3 feels that this need is not adequately addressed in the current proposal [1], [2]:

- LCS client, service, and requestor are identified by "MSISDN or logical name", which both can be spoofed.

- Requestor shall authenticate with a "codeword". Besides providing only weak authentication in terms of security, password schemes have proven to be both vulnerable and user-unfriendly.

Proposed actions for SA1 and SA2:

SA3 proposes the following actions for SA1 and SA2. SA3 is willing give support regarding all security related issues.

1. Trust and Security Model

Before defining a security model, SA1/2 should define a trust model for LCS. The trust model usually follows the business model (who bills the user's bank account?). For example, it may be more straightforward for the user to trust one GMLC operator than a multitude of VASPs.

A trust model is a prerequisite for identifying threats and security requirements.

2. Le Interface Security (LCS Client – LCS Server)

LCS client and server have a trust relationship which is reflected in a contract. SA1/2 should define adequate security requirements for this interface. To protect users' location data, the channel must provide

- mutual authentication

- integrity protection

- confidentiality

SA3 is willing to help selecting the appropriate protocol security. Inviting LCS experts to SA3 meeting would be helpful in discussing the architecture and the trustmodel. ??

3. Requestor Authentication

SA3 believes that SA1/2 should reconsider the "codeword" for requestor authentication. From a user's perspective it is very inconvenient to manage many codewords for multiple services and multiple requestor groups – both for the user to be located and for the requestors. Furthermore, the provided authentication is believed not to be adequate to the delicate LCS issue. SA3 suggests using a strong authentication mechanism

In any case, confidentiality of codewords has to be guaranteed while passing insecure networks and several involved parties. This might not be easy to achieve.

4. Interface LCS Client – Requestor

SA1/2 should consider privacy of location data travelling from LCS client to the requestor. Even if a subscriber agrees to reveal his location to a specified requestor, he does not implicitly agree to send this information via insecure channels (e.g. sending it to the requestor via the Internet as clear text). SA1/2 should specify (security requirements for) this interface.

5. Interoperability

SA1/2 should pay attention to the work going on in IETF [3] – if not known yet.

References:

[1]   S2-020316 containing 23.871 Ver. 1.10

[2]   S1-020422 containing "codeword" CR to 22.071

 [3]   ??? IETF draft on GEO priv

Date of Next SA3 Meetings:

SA3_23   14th – 16th May 2002   Victoria Island, Canada