3GPP TSG SA WG3 #22 Tdoc S3-020145

Bristol, UK
25th February – 28th February 2002

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 SA3 defines 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. To protect users’ location data, the channel must provide:

- mutual authentication

- integrity protection
- confidentiality

SA3 is willing to select the appropriate security protocol.

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.

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). The security requirements for this interface needs to be clarified.

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] http://www.ietf.org/html.charter/geopriv-charter.html

Actions:

SA1, SA2: SA3 would like to invite LCS experts to the SA3 meeting in Victoria Island, Canada, to discuss the architecture and the trust model.

Date of Next SA3 Meetings:

SA3_23	14th – 17th May 2002	Victoria Island, Canada