3GPP TSG SA WG3 Security — S3#23 **S3-020193**
14 - 17 May 2002
Victoria, Canada

TSG-SA WG 1 SWG LCS meeting **S1-020860**
Sophia-Antipolis, France, 11 April 2002

Response liaison statement

Title: **Response LS to SA3 on new security requirements for LCS**
Source: **SA1**
To: **SA3, SA2, LIF, CN5**
CC:

Contact Person:
Name: Tommi Kokkola
Tel. Number: +358 40 5040734
E-mail Address: **tommi.kokkola@nokia.com**

Attachments: LS from SA3 (S3-020145)

1. Overall Description:

This LS is a reply to SA WG3's LS S1-020687 (S3-020145). SA1 thanks SA3 for the information given regarding the security aspects of the enhanced support for user privacy in location services. SA1 agrees with SA3 that location information is a delicate issue from user privacy and security points of view.

1.1 Trust and security model

SA1 has specified service requirements for the requestor, LCS client, LCS server and e.g. requirements to protect the privacy of the target mobile user. The security aspects of LCS are specified in TS22.071, chapter 4.7 and the privacy aspects of LCS in chapter 4.8. The latest version 5.1.1 of TS22.071 includes new requirements on user privacy for Rel-5. SA3 is invited to study TS 22.071 in order to determine whether further changes would be needed.

1.2 Le interface security

SA1 shares SA3's concern on this issue but SA1 believes that overall service requirements in this area are already specified.

1.3 Requestor Authentication

The codeword mechanism, as currently described in TS 22.071, is intended to be used for authorisation and not authentication. SA1 recognise that the current service requirement may be difficult to handle for the target mobile user and for the requestors. SA1 would be happy to enhance this functionality for Rel-6 and invites SA3 to propose improvements.

1.4 Interface LCS Client – Requestor

The current approach in SA1 and SA2 is to leave the LCS client – requestor interface un-standardized, because the interface is seen to be application related and outside the scope of 3GPP. This approach could be reconsidered if seen necessary.
SA3 is invited to provide recommendations on the security requirements for the LCS client – requestor interface.

1.5 Interoperability

SA1 thanks SA3 for the information on the IETF activities regarding spatial information. In addition it is noted that LIF and possibly other bodies are developing open standards that are relevant for security aspects that may be related to location services.

2. Actions:

SA1 kindly invites LIF to study the security aspects and requirements for the requestor - LCS client – GMLC interfaces as reflected in the SA3 LS and also kindly requests SA2 to verify whether SA2 shares the views of SA1 on this issue. SA3 is kindly requested to check the security and privacy requirements in TS22.071 and give guidance on possible improvements and to provide recommendations on the security requirements for the LCS client – requestor interface. CN5 is kindly requested to participate in this issue and review any future proposals from LIF.

3. Date of Next SA1 Meetings:

Title	Date	Location	Country
SA1#16	13 – 17 May 02	Victoria	Canada
SA1 Adhocs	8 – 12 Jul 02	Rome	Italy
SA1#17	12 – 16 Aug 02	To be determined	North America
SA1 Adhocs	14 - 18 Oct 02		
SA1#18	11-15 Nov 02		

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