3GPP TSG SA WG3 Security — S3#23 **S3-020302**
14 - 17 May 2002
Victoria, Canada

Title:	[DRAFT] Response LS to SA1 and SA2 on security and enhanced user privacy requirements for LCS
Response to:	LS S1-020860 (S3-020193) from SA1 and S2-021466 (S3-020195) from SA2
Source:	TSG-SA WG3
To:	TSG-SA WG1, TSG-SA WG2
Cc:	??? CN5, LIF ???

Contact Person:

Name:	**Stefan Schröder**
Tel. Number:	+49 228 936 3312
E-mail Address:	stefan.schroeder@t-mobile.de

1. Overall Description:

SA3 thanks SA1 and SA2 for the LSes listed above. The topics mentioned in this LS have been discussed during a joint meeting of SA1 and SA3 in Victoria. SA3 agreed to collect the statements and elaborate them within an LS to allow SA1 considering these issues offline. Some issues were identified which relate to SA2 work, so this reply is sent to both groups to reach a common understanding while considering the ACTIONS suggested below.

1.1 Trust and security model

SA3 studied TS 22.071 V5.1.1 as suggested. Some issues have been identified, which should be addressed in the TS:

a) A **trust model** should clearly identify the parties involved and the network elements representing the parties for *all* scenarios in the scope of the TS. The network entities should be clearly distinguished from the parties they belong to. All NE needed to define the trust model should be reflected in the architectural model defined by SA2 (e.g. in figure 6.1 of TS 23.271). Furthermore, definition of the trust model should be consistent in the use of terms. Suggestion for definition of parties and NE:

Parties:	HPLMN operator, VPLMN operator, VASPs contracted with HPLMN operator, VASPs contracted with VPLMN operator, Requestor, Target UE owner, others?
NE:	LCS Client, LCS Server, LCS capable PLMN, Requestor Terminal, Target UE, others?

One example which kind of clarification is needed: clause 4.7 of TS22.071 says in the general part "The LCS client MAY be authorized by the LCS Server", but later on says that for VASPs "Only authorized LCS Clients SHALL be able to access the LCS server". To SA3's view, it is not clearly defined when authorization is optional and when it is required considering the complete list of parties in the trust model.
A second example: To SA3's understanding it is not clear what "PLMN operator services" (same clause) mean for the trust model (probably "LCS client, server, and Requestor terminal owned by the same PLMN operator"?).

b) TS 22.071 should clearly state in consistent terms which **security services** are required for which trust scenario. Clause 4.7 of TS22.071 uses the term "secure and reliable manner, such that the location information is neither lost, corrupted nor made available to any unauthorized third party" and sub-parts of this term. SA3 suggests that SA1 uses the following terms to define security services required for *all* scenarios in the scope of the TS, clearly identifying possibly different requirements depending on the parties involved:

- integrity protection
- confidentiality protection
- (mutual) authentication

In addition, the requirement "reliable manner" and "information is not lost" should be moved from definition of security requirements to clause 4.4 (Reliability).

c) Similar to b), the **privacy requirements** of clause 4.8 of TS22.071 should be clearly related to the parties involved. From the current text, it is not clear when requirements are general, related to a PLMN operator, a VASP or any other party. Requirements are mixed but it is not obvious which requirement supersedes another.

d) The privacy clause 4.8 of TS22.071 should clearly state which information should be hidden from which parties. The current TS seems to refer to privacy of the *Target UE's position information*, while TR 23.871 additionally introduces the privacy requirement of the *Target UE owner's identity* (anonymity). Other privacy requirements may also be necessary.

e) SA3 suggests that all LCS security related requirements be located within a single clause of a single TS. Currently, security requirements are spread within TS 22.071: clause 6.5 duplicates part of clause 4.7 and introduces a new requirement (see f)); clause 6.4.6 introduces new requirements, e.g. that a Requestor SHALL be authenticated. Furhermore, TR 23.871 introduces other requirements (see d)).

f) Clause 6.5 of TS22.071 refers the information "point of origin of location request". Does this mean "Requestor identity"? Regarding this information, please see also section 1.3 b) below.

g) SA3 suggests that SA1 and SA2 adopt key word definitions of RFC2119 when defining requirements. Re-phrasing the RFC slightly to explain the reason:

```
   Key words are frequently used to specify behavior with security
   implications.  The effects on security of not implementing a MUST or
   SHOULD, or doing something the specification says MUST NOT or SHOULD
   NOT be done may be very subtle. Document authors should take the time
   to elaborate the security implications of not following
   recommendations or requirements as most implementors will not have
   had the benefit of the experience and discussion that produced the
   specification.
```

That way, potentially misleading terms like "SHALL OPTIONALLY" in clause 6.4.6 of TS22.071 can be avoided.

h) In addition to g), SA3 suggests that SA1 and SA2 adopt a more structured way of defining conditional requirements like "IF <OPTIONAL feature> is implemented, THEN <other feature> MUST also be implemented". This may apply to clause 6.4.6 of TS22.071, and probably others.

1.2 Le Interface Security

Provided that the ideas of section 1.1 are incorporated into TS 22.071, SA3 shares SA1's view that Le interface security requirements are adequately defined.
SA3's current understanding is that the Le interface may be based on OSA. However, OSA is a functional framework rather than a full interface specification. If middleware and communication protocols for Le below OSA are left for the implementor to choose, it is also up to the implementor to meet security requirements. In this case SA3 can not contribute anything more than the high level requirements pointed out in section 1.1 However, a vendor specific Le interface may be undesirable for 3GPP because it limits interoperability when interconnecting multiple LCS Clients with multiple LCS Servers.
SA3 kindly asks SA2 whether security requirements (once they are refined) can be met in the architecture and to what detail the Le interface will be specified.

1.3 Requestor Authentication

a) In the joint session it was clarified that current LCS specifications should clearly distinguish authorization (giving defined rights to an entity) from authentication (verifying the identity of an entity). Usually it makes no sense to provide authorization without authentication. SA1 and SA2 are kindly requested to verify if their current specifications correcly reflect their requirements. Clauses 8.1 and 8.2 of TR 23.871, for example, seem to mix both terms up.

b) SA3 feels that SA1 should clearly define where a location request may originate (Requestor Terminal network connection). Without explicitly stating it, current LCS specifications of SA1 and SA2 seem to assume that the Requestor terminal is always a PLMN UE (e.g. by suggesting the MSISDN as Requestor identity). However, already today some LBS exist which can be requested via the Internet – so this should also be considered. This definition is important because it may influence design of architecture and authentication framework.

c) Common understanding of the codeword mechanism is that it may not be optimal but it is too late to improve it for Rel. 5. SA3 thinks it might be a better approach for future releases that SA1 defines the requirements

rather than a mechanism (or the solution) and lets SA2 and SA3 decide on the adequate architecture and security mechanisms to meet those requirements.
Once trust relations according to section 1.1 above are defined by SA1, the codeword mechanism might show not adequate to these requirements. The codeword might be meant to enable one Requestor to locate a specific Target, but not to enable that Requestor sharing this right with others (what it actually does, too).

1.4 Interface LCS Client - Requestor

SA1 understands SA1's motivation to define this interface as out of scope. This interface, however, carries the same sensitive information than the Le interface – so the same requirements should apply. The importance of the Requestor is already reflected by including Requestor Authentication into SA1 and SA2 specifications, while the interface itself is still defined as out of scope.
Location information leak due to inadequate security requirements on this interface may render security of the remaining LCS system useless. Furthermore, the connection may be eavesdropped revealing the codeword, if confidentiality is not required. If mutual authentication is not required, a fake LCS client may be set up to collect codewords.
SA3 kindly asks SA1 to at least define high-level security requirements for this interface as guidelines for implementors. There may already be requirements on this interface defined by other groups (LIF, GEOPRIV?) so that this workload may be minimized to a referral.

2. Actions:

To SA1 and SA2

ACTION: SA3 kindly asks SA1 and SA2 to address the issues above in their LCS-related specifications for Release 6

3. Date of Next TSG-SA3 Meetings:

TSG-??? Meeting #n	9th – 13th July 2001	Dresden, Germany.
TSG-??? Meeting #n+1	15th – 19th October 2001	U.K.