**3GPP TSG SA WG3 Security — S3#33** **S3-040365**
**10 - 14 May 2004**
**Beijing, China**

Technical Specification Group GERAN **TSGG#19(04)1195**
Meeting #19, Cancun, Mexico, 19-22 April 2004

**Title:** ***Use of Kc in the Uplink TDOA location method***

**Release:** Release 6

**Source:** GERAN
**To:** SA3

**Contact Person:** TruePosition
**Name:** Bob Gross
**Tel. Number:** +1-610-680-1119
**E-mail Address:** rlgross@trueposition.com

### 1. Overview

GERAN would like to thank SA3 for the LS in S3-040152 "Reply LS on security recommendations for the protection of Kc in the Uplink TDOA location method". SA3's recommendations have been included in CR 043 to TS 43.059 v6.2.0 in paragraph 9.5.1.2. As discussed in SA3 #32 in Edinburgh, this CR has been posted on the SA3 reflector for review during the period of 2-16 April 2004.

### 2. Actions for the SA3:

As requested by SA3 in the LS S3-040152, GERAN seeks SA3's review and endorsement of the attached CR 043 to TS 43.059 (GP-040634).

### 3. Date of Next TSG-GERAN Meetings:

| Meeting | Date | Location |
|---|---|---|
| G2#19 bis | 24-28 May, 2004 | Sophia Antipolis, France |
| GERAN#20 | 21-25 June, 2004 | Bilbao, Spain |

*CR-Form-v7*

# CHANGE REQUEST

⌘ **43.059** **CR** **043** ⌘ **rev** **2** ⌘ Current version: **6.2.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

***Proposed change affects:*** UICC apps⌘ [ ] ME [ ] Radio Access Network [X] Core Network [ ]

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Removal of emergency services client type restriction from the U-TDOA location method |
| ***Source:*** | ⌘ | Cingular Wireless, T-Mobile, Andrew Corporation, and TruePosition |
| ***Work item code:*** | ⌘ | UTDOA-CS |
| ***Date:*** | ⌘ | 4/19/2004 |
| ***Category:*** | ⌘ | C |
| ***Release:*** | ⌘ | Rel-6 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*

| | |
|---|---|
| *2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | To allow the U-TDOA location method to be applied to all location based services. This restriction should be removed to include all client types specified in LCS stage 1 specification TS 22.071. |
| ***Summary of change:*** | ⌘ | Removal of phrase restricting the provision of Kc to emergency calls for the U-TDOA location method. |
| ***Consequences if not approved:*** | ⌘ | It will not be possible to apply the U-TDOA location method to AMR calls and will require more system resources for U-TDOA location based services |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | 9.5, 9.5.1.2 |

| ***Other specs affected:*** ⌘ | Y | N | | ⌘ |
|---|---|---|---|---|
| | | X | Other core specifications | |
| | | X | Test specifications | |
| | | X | O&M Specifications | |

***Other comments:*** ⌘

**How to create CRs using this form:**
Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.
2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.
3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

**<First changed section>**

# 9.5 U-TDOA Positioning Procedures

## 9.5.0 General

Following the receipt of a location request message from the BSC, the U-TDOA capable SMLC interrogates the BSS for the RF channel information associated with the MS to be located. The SMLC uses this information to task the LMUs at the serving and surrounding cells. The LMUs are tasked to measure the identified RF channel(s) and thus provide a time reference from different LMUs. The time-of-arrival information from the tasked LMUs is returned to the SMLC where the MS location is calculated.

## 9.5.1 U-TDOA Positioning in CS Domain for A/Gb-mode

### 9.5.1.1 General Procedures

The U-TDOA location method uses the uplink energy transmitted by an MS to make a location determination. If the MS was in the dedicated mode, carrying subscriber traffic prior to the beginning of the location process, the energy associated with this subscriber traffic can be used to locate the MS. If the MS was placed in the dedicated mode by the MSC specifically for location determination purposes, either the SDCCH or TCH can be used for U-TDOA location purposes.

### 9.5.1.2 U-TDOA Messages and Procedures on the Lb Interface

The following section describes the positioning procedure for U-TDOA location determination on the Lb interface.

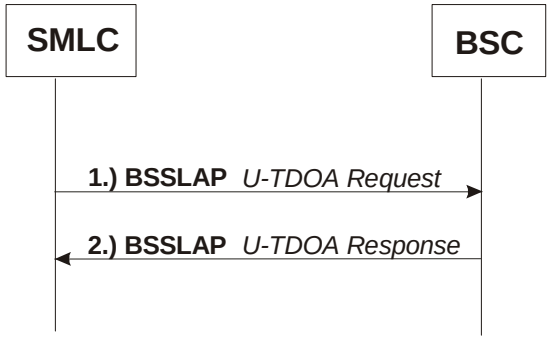


**Figure 36: U-TDOA Positioning Procedure**

1. The SMLC sends a BSSMAP-LE Connection Oriented Information message to the BSC that contains the embedded BSSLAP U-TDOA Request message. The U-TDOA Request message may contain the delta timer value. The BSC starts the delta timer, received or internal, immediately after sending the U-TDOA Response message to the SMLC. The purpose of this timer is to define the maximum time during which the BSC supervises the location request.

2. The BSC sends a BSSMAP-LE Connection Oriented Information message to the SMLC that contains the embedded BSSLAP U-TDOA Response message. The U-TDOA Response message contains; the physical channel information (frequencies, hopping sequence, channel type, time slot, sub-channel number, etc.); the MS power; the cell identifier; and the TA. If frequency hopping is used, the U-TDOA Response message also includes the frequency list. ~~For all U-TDOA positioning procedures related to emergency services, t~~The U-TDOA Response message ~~shall~~ also contains the ~~encryption~~ ciphering key (Kc) if ~~encryption~~ ciphering is used on the air interface and the version of the applied A5 ~~encryption~~ ciphering algorithm (A5/x). The Kc is ciphered if sent from the SMLC to any LMU. The SMLC and any LMU with which it interacts shall also be mutually authenticated. These requirements shall be met using a security mechanism meeting the capabilities of the Zb interface of NDS/IP (TS 33.210) or TLS (RFC 2246). The LMU installation shall meet the same physical

security requirements as a BTS installation. For ~~emergency services calls~~locations on channels that are not ~~encrypted~~ciphered, the algorithm identifier will show the same. ~~The above mentioned items constitute a channel description for U-TDOA purposes.~~