**3GPP TSG SA WG3 Security — S3#32** **S3-040145**
**9-13 February 2004**
**Edinburgh, Scotland**

**Title:** **Reply LS on security recommendations for the protection of Kc in the Uplink TDOA location method**

**Response to:** **GP- 040561**

**Source:** **SA3**

**To:** **TSG GERAN**

**Cc:**

**Contact Person:**
**Name:**
**Tel. Number:**
**E-mail Address:**

## 1 Introduction

SA3 would like to thank GERAN for the LS in GP-040561 "Protection of Kc in the Uplink TDOA location method". SA3 has considered this LS together with a related presentation from TruePosition and Andrew Corporation provided to SA3 in S3-040146.

SA3 has studied the Uplink TDOA method where the Kc is distributed from the SMLC to co-operating LMUs so that bursts from the mobile can be decrypted to enable the location of MS using AMR, increased location accuracy and reduced data volume. SA3's security recommendations for the protection of Kc are described in section 2.

## 2 Security recommendations for the protection of Kc in the Uplink TDOA location method

Use of the Kc in the Uplink TDOA location method requires protection of the Kc during transport from the SMLC to the LMUs and physical protection of the LMUs.

### 2.1 Protection of Kc during transport

The Kc must be encrypted during the transport from the SMLC to all LMUs using, as a minimum, the Secure Socket Layer encryption method.

### 2.2 Physical protection of Kc

The LMU installation must meet, as a minimum, the same physical security requirements as a BTS installation.

## 3 Summary

It is suggested that additional security measures are needed to compensate for the increased exposure of the Kc as described in Section 2 of this document.

## 4 Actions for GERAN

GERAN is asked to implement the above security recommendations for the Uplink TDOA method by including them in the appropriate GERAN specification(s).

## 5 Next SA3 Meetings

| Meeting | Date | Location |
|---|---|---|
| SA3 #33 | 11-14 May 2004 | Beijing, China |
| SA3 #34 | 6-9 July 2004 | Chicago, USA |