

# Kc security for the U-TDOA LCS method

S3-040146

SA3 #32 – Edinburgh, Scotland

February 9-13, 2004

## History of the U-TDOA Kc effort

- GERAN #13 in San Antonio, Texas February 2003
  - LS to SA3 (GP-030451) asking for evaluation of the security impact of using Kc for U-TDOA
- SA3 #27 in Sophia-Antipolis February 2003
  - Presentation of GERAN LS to SA3 (S3-030038) and LS reply to GERAN (S3-030152)
- GERAN #14 in Munich April 2003
  - Presentation of SA3 LS (GP-030477)
  - GERAN asked for clarification of SA3's security concerns and recommendation of potential solutions.
- SA3 #28 in Berlin May 2003
  - TruePosition presentation (S3-030196) recommends the use of Diffie-Hellman key agreement protocol. Secure Socket Layer (SSL) protocol was recommended.
  - The Chairman suggested that a LS from GERAN was appropriate
- GERAN #18 in Reykjavik February 2004
  - LS to SA3 (GP-040561) asking for security recommendation

# GERAN Request

- GERAN requests security recommendation for the use of  $K_c$  for the U-TDOA location method
- LS to GERAN
  - Encryption recommendation for  $K_c$  when transported between the SMLC and LMUs
    - SSL?
  - Physical Security recommendation
    - Same as BTS?