3GPP TSG SA WG3 Security — S3#31 **S3-030668**
18 - 21 November 2003
Munich, Germany

3GPP TSG-CN1 Meeting #32 Tdoc N1-031612
Bangkok, Thailand, 27 – 31 October 2003

Title: Reply LS on Special-RAND mechanism
Response to: LS (S3-030652 / N1-031462) from SA3 on Special-RAND mechanism
Release: Rel-6

Source: CN1
To: SA3
Cc: GERAN 2

Contact Person:
Name: Robert Zaus
Tel. Number: +49 89 63675206
E-mail Address: robert.zaus@siemens.com

Attachments: ---

1. Overall Description:

CN1 would like to thank SA3 for their LS on the Special-RAND mechanism.

CN1 briefly discussed the proposed special-RAND mechanism described in clause 2 of Tdoc S3-030651and agreed that it looks feasible.

Furthermore, CN1 would like to comment on the analysis in subclause 3.2.2 of the same document:

> 3.2.2 GSM packet switched
>
> It should be considered what happens when a Special RAND capable mobile receives an AUTHENTICATION AND CIPHERING REQUEST instructing it to start ciphering using an algorithm that is forbidden to be used with the current cipher key. It is proposed that the GMM layer in the mobile treats this as an error case and does not start ciphering uplink traffic at the LLC layer [24.008, 43.020]. Since the SGSN is expecting uplink traffic to be encrypted it will result in a layer 2 failure in the SGSN.
>
> In summary no special error handling needs to be specified.

and to ask SA3 for guidance on the following issues:

1) On the Gb interface it is possible to perform authentication and start ciphering with one procedure, by including both a RAND and an appropriate ciphering algorithm in the AUTHENTICATION AND CIPHERING REQUEST message.

   If the authentication challenge is a UMTS authentication and the message contains:
   - both an authentication failure (MAC failure or Synch failure) and
   - a ciphering algorithm that is not permitted according to the special-RAND information,

   which error takes precedence? Should the UE report an Authentication and Ciphering Failure to the network or should it diagnose a 'not permitted ciphering algorithm' first and skip the authentication?

2) If the GMM layer in the UE is required to treat the request for a 'not permitted ciphering algorithm' as an error, the UE should not return an AUTHENTICATION AND CIPHERING RESPONSE message. According to TS 24.008 (subclause 4.7.7.3), however, without receipt of an AUTHENTICATION AND CIPHERING RESPONSE message the SGSN will not start ciphering. I.e. the layer 2 failure mentioned

in the above scenario will not occur.

CN1 noted that possible candidates for an explicit error indication by the UE to the SGSN would be the GMM STATUS or the AUTHENTICATION AND CIPHERING FAILURE message, but did not discuss this in detail.

3) When it is proposed that the UE shall not start ciphering the uplink traffic at the LLC layer, what kind of traffic is the UE allowed to send in the uplink – signalling and/or user data, or none at all?

4) Finally, what is the expected UE reaction after detection of a 'not permitted ciphering algorithm' error?
   - Bar the cell, as in the case the network fails a UMTS authentication procedure (TS 24.008, subclause 4.7.7.6.1)?
   - Deactivate all active PDP contexts?
   - Perform a detach from the network?
   - Or any combination of these measures?

2. Actions:

To SA3 group.

ACTION: CN1 kindly asks SA3 to provide answers to the above questions so that CN1 can get a better understanding of the requirements.

3. Date of Next TSG-CN1 Meetings:

CN1_33	16th – 20th February 2004	Atlanta, USA (NA friends of 3GPP)
CN1_34	10th – 14st May 2004	TBD, Croatia (EF3)