3GPP TSG SA WG3 Security — S3#13 **S3-000327**

23-26 May, 2000

Yokohama, Japan

Source: Gemplus

Title: **Clarification on UMTS AKA for GSM R'99 mobiles.**

Document for: Discussion 3GPP S3 / EP SMG9 / 3GPP T3

Introduction:

When reading 3G TS 24.008 (CN1), 3G TS 33.102 (S3), GSM 11.11 R'99, the following ambiguity appears :
does a GSM R'99 mobile need to support the 3G authentication and key agreement (3G AKA) ?

Problem:

In 3G TS 24.008 v3.2.1, clause 4.3.2.5.1 :
"*A R99 GSM-only MS connected to a R99 core network (even using the BSS radio access) shall support a UMTS authentication challenge*."

same specification, clause 4.7.7a :
"A R99 GPRS-only MS connected to a R99 core network (even using the BSS radio access) shall support a UMTS authentication challenge."

In 3G TS 33.102 v3.4.0, clause 6.8.1.1 :
"For UMTS subscribers, authentication and key agreement will be performed as follows:

- *UMTS AKA shall be applied when the user is attached to a UTRAN.*
- *UMTS AKA shall be applied when the user is attached to a GSM BSS, in case the user has R99+ UE and also the VLR/SGSN is R99+. In this case, the GSM cipher key Kc is derived from the UMTS cipher/integrity keys CK and IK, by the VLR/SGSN on the network side and by the USIM on the user side.*
- *GSM AKA shall be applied when the user is attached to a GSM BSS, in case the user has R98- UE. In this case, the GSM user response SRES and the GSM cipher key Kc are derived from the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. A R98- VLR/SGSN uses the stored Kc and RES and a R99+ VLR/SGSN derives the SRES from RES and Kc from CK, IK.*

NOTE: To support R98- UE the UICC may contain a GSM SIM application which provides the corresponding GSM functionality for calculating SRES and Kc based on the 3G authentication key K and the 3G authentication algorithm implemented in the USIM. Due to the fact that the 3G authentication algorithm only computes CK/IK and RES, conversion of CK/IK to Kc shall be achieved by using the conversion function c3, and conversion of RES to SRES by c2."

Note that in 3G TS 33.102, if a "R98- UE" is clearly a GSM-only R'98 ME, it is not said what is a "R99+ UE".

In GSM 11.11 v8.2.0 (SIM specification R'99): nothing about the support of UMTS AKA.

Conclusion

Either what is desired is the support of UMTS AKA for GSM R'99 ME :

- one possibility is to include the UMTS AKA commands in GSM 11.11 R'99
- another possibility is to mandate the support of UICC/USIM for GSM R'99 terminals

either what is desired is the support of UMTS AKA only for 3G ME :

- 3G TS 24.008 has to be corrected
- In 3G TS 33.102, "R98- UE" can be replaced by "GSM ME" and "R99+ UE" by "3G ME"

3GPP-T3 and S3, EP SMG9 are kindly invited to clarify the issue.