3GPP TSG SA WG3 Security — S3#13 **S3-000338**

23-26 May, 2000

Yokohama, Japan

Source: **Ericsson**

Title: **GSM AKA and conversion function c3**

Document for: **Discussion**

Agenda Item: **TBD**

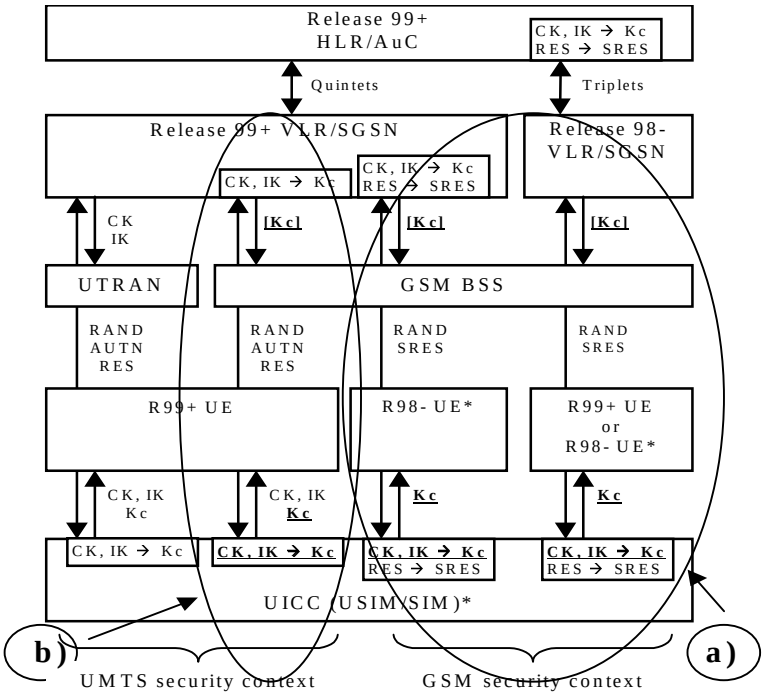
---

1. Introduction

This contribution seeks for a common understanding on the support of conversion function c3 at the UICC in relation with the support of GSM AKA. The real implications depending on whether these functions are supported or not at the UICC are also depicted.

2. Need for conversion function c3

Conversion function c3 is required at the UICC to derive GSM Kc from UMTS CK and IK for a UMTS subscriber in the following cases:



a) GSM security context must be applied, i.e. the UMTS subscriber is under a R98- VLR/SGSN and/or with a R98- UE. In this case, full support of GSM AKA at the UICC is required (both conversion functions c2 and c3 are required).

b) UMTS security context must be applied under GSM-BSS, i.e. the UMTS subscriber is under a R99+ VLR/SGSN with a R99+ UE. In this case, support of GSM AKA at the UICC is not required (support of conversion function c2 is not needed), but support of conversion function c3 is still required to derive and apply GSM Kc under GSM-BSS.

According to TS 33.102 v3.4.0, it can be inferred that the support of conversion function c3 is conditioned to the support of GSM AKA:

> *"…If the sequence number is considered to be in the correct range however, the USIM computes RES = $f2_K$ (RAND) and includes this parameter in a user authentication response back to the VLR/SGSN. Finally the USIM computes the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.* ***If the USIM also supports GSM AKA, it shall derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3****. UMTS keys are sent to the MS along with the derived GSM key for UMTS-GSM interoperability purposes. USIM shall store original CK, IK until the next successful execution of AKA. The USIM also stores RAND until completion of the current AKA, for re-synchronisation purposes…"*
>
> *"…When the UE provides the UICC with only RAND,* ***GSM AKA shall be executed, if supported****. The UICC first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK.* ***The UICC then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3.*** *The UICC then stores the GSM cipher key Kc and sends the GSM user response SRES and the GSM cipher key Kc to the UE.*
>
> *"…****In case the UICC does not support GSM AKA (conversion function c3 is not available to derive Kc and pass it to the R99+ UE), the R99+ UE shall be informed****. A UICC that does not support GSM AKA cannot operate under a R98- VLR/SGSN or in a R98- UE.*

3. **Conclusion**

If this assumption is correct, when the UICC does not support GSM AKA, then conversion function c3 is not available at the UICC to derive and apply GSM Kc after UMTS AKA is executed for a UMTS subscriber under GSM-BSS.

The real effect for a UICC not supporting GSM AKA (and consequently not supporting conversion function c3) is that the UICC can not operate under GSM-BSS, it can only operate under UTRAN.

The attached CR presented for S3 consideration and approval, updates TS 33.102 accordingly.

3GPP TSG SA WG 3 (Security) meeting #13
Yokohama (Japan), 24—26 May, 2000

Document **S3-000338_Attach**
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102	**CR**	**xxx**	Current Version:	3.4.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to:	SA #8	for approval	X	strategic		(for SMG use only)
list expected approval meeting # here ↑		for information		non-strategic		

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc*

Proposed change affects: *(at least one should be marked with an X)* (U)SIM [ ] ME [ ] UTRAN / Radio [ ] Core Network [X]

Source: Ericsson **Date:** 2000-05-19

Subject: UICC support of GSM AKA and/or c3 conversion function.

Work item: Security

Category: *(only one category shall be marked with an X)*

F	Correction	X	**Release:**	Phase 2	
A	Corresponds to a correction in an earlier release			Release 96	
B	Addition of feature			Release 97	
C	Functional modification of feature			Release 98	
D	Editorial modification			Release 99	X
				Release 00	

Reason for change: Since the support of conversion function at the UICC is conditional to the support of GSM AKA, a UICC that does not support GSM AKA cannot operate under GSM-BSS (it can only operate under UTRAN).

Clauses affected: 6.8.1.4, 6.8.1.5.

Other specs affected:

Other 3G core specifications	[ ]	→ List of CRs:
Other GSM core specifications	[ ]	→ List of CRs:
MS test specifications	[ ]	→ List of CRs:
BSS test specifications	[ ]	→ List of CRs:
O&M specifications	[ ]	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR

6.8.1.4 R99+ UE

R99+ UE with a USIM inserted and attached to a UTRAN shall only participate in UMTS AKA and shall not participate in GSM AKA.

R99+ UE with a USIM inserted and attached to a GSM BSS shall participate in UMTS AKA and may participate in GSM AKA. Participation in GSM AKA is required to allow registration in a R98- VLR/SGSN.

The execution of UMTS AKA results in the establishment of a UMTS security context; the UMTS cipher/integrity keys CK and IK and the key set identifier KSI are passed to the UE. If the UICC also supports GSM AKA, ~~T~~the UE shall also receive a GSM cipher key Kc derived at the USIM.

The execution of GSM AKA results in the establishment of a GSM security context; the GSM cipher key Kc and the cipher key sequence number CKSN are stored in the UE.

6.8.1.5 UICC (USIM/SIM)

The UICC shall support UMTS AKA (UICC shall contain USIM application) and may support GSM AKA (UICC may contain a SIM application). Support of GSM AKA is required to allow access to GSM-BSS with a R98- VLR/SGSN and/or with a R98- UE.

When the UE provides the UICC with RAND and AUTN, UMTS AKA shall be executed. If the verification of AUTN is successful, the UICC shall respond with the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The UICC shall store CK and IK as current security context data. The UICC shall also derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3 and send the derived Kc to the R99+ UE. In case the verification of AUTN is not successful, the UICC shall respond with an appropriate error indication to the R99+ UE.

When the UE provides the UICC with only RAND, GSM AKA shall be executed, if supported. The UICC first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The UICC then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The UICC then stores the GSM cipher key Kc and sends the GSM user response SRES and the GSM cipher key Kc to the UE.

In case the UICC does not support GSM AKA (conversion function c3 is not available to derive Kc and pass it to the R99+ UE), the R99+ UE shall be informed. A UICC that does not support GSM AKA cannot operate under GSM-BSS, it can only operate under UTRAN. ~~a R98- VLR/SGSN or in a R98- UE~~.