3GPP TSG SA WG3 Security — S3#14 **S3-000428**

2-4 August, 2000

Oslo, Norway

Source: **Gemplus**

Title: Interactions between a user identity mobile (SIM or USIM) and a phone (ME)

Document for: **Information**

Agenda Item:

1 Introduction

This document describes the different cases of interaction between an Identity Module (GSM SIM or 3G USIM) and a Mobile Equipment (GSM or 3G phone). Cases not described here should be seen as not supported.

2 Case of a SIM

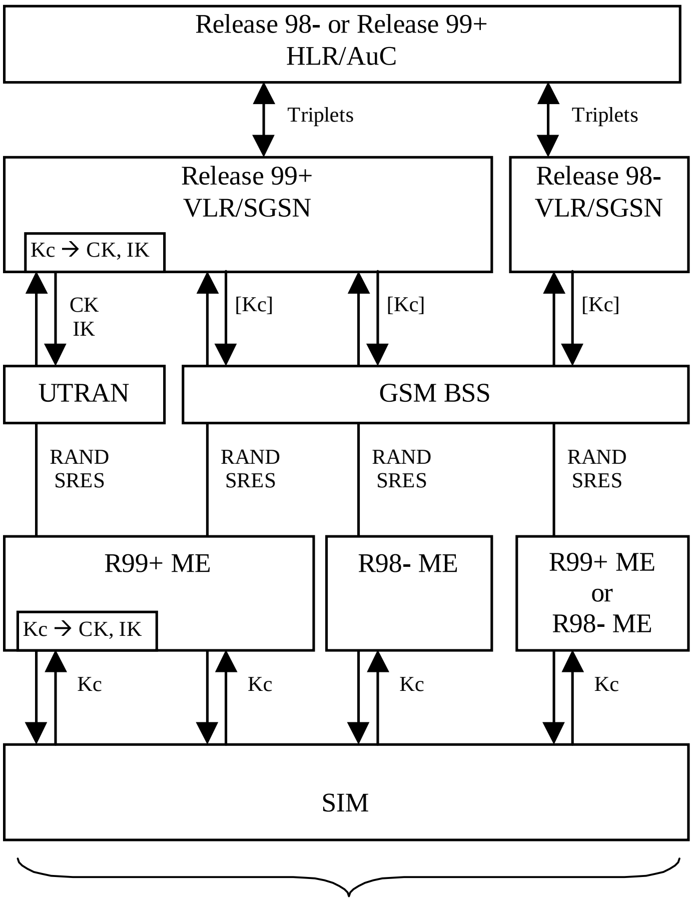
The ME can be either a R98- or R99+.

The SIM receives RAND and sends Kc and SRES.

A UICC (release 99+) may emulate a SIM. In this case the emulation is started when the smart card receives the first command. This first command received by the smartcard is used to detect the operational mode of the UICC. If the first command is a GSM 11.11 command the GSM emulation is started. The SIM emulation goes on until the card is power down.

The SIM does only use the GSM 11.11 set of commands, even if it is a SIM emulated by a USIM. A SIM does not recognise any USIM command.

No change with 33.102 v3.4.0 chapter 6.8.2.1 for the diagram (except UE changed to ME)



GSM security context

3 Case of a USIM

The USIM receives RAND, AUTN and sends (IK, CK) and RES using the AUTHENTICATE command, see 7.1 AUTHENTICATE.

The USIM command AUTHENTICATE *may* be used to derive Kc
The USIM command AUTHENTICATE *may* be used to derive SRES

TSG WG SA3 decided to separate those two commands.

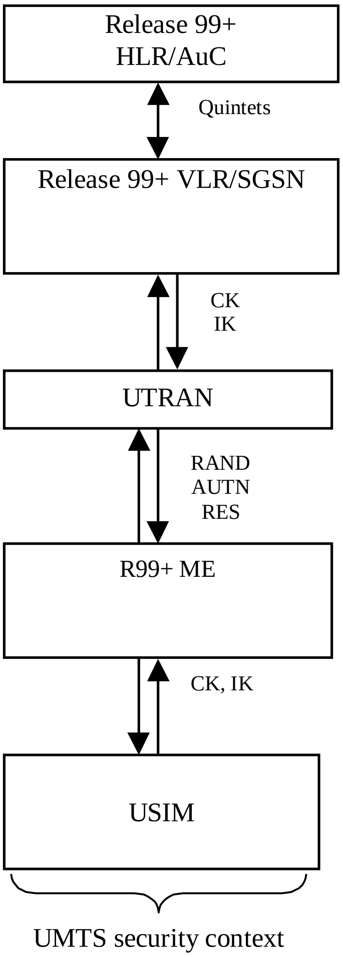
A USIM does only use the 3G set of commands. GSM 11.11 commands are not available.

The following parts describes the different cases:

1. pure 3G mode
2. 3G + SRES generation (function c2)
3. 3G + Kc generation (function c3)
4. 3G + SRES + Kc (functions c2 and c3)

3.1 USIM only

Only the 3G authentication is possible.

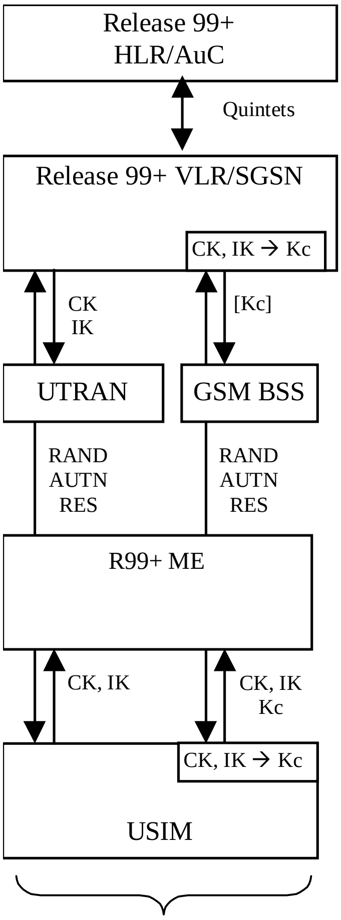


3.2 USIM with function c2

The function c2 is used to convert UMTS RES to GSM SRES.
In the present case the USIM does not have the function c3; so the ME does not have access to the GSM key Kc.
The mobile cannot use a GSM BSS. This situation is the same as in the previous case (USIM only) and only the 3G authentication is possible.

3.3 USIM with function c3

The function c3 is used to convert UMTS CK, IK to GSM Kc
The ME cannot be a R98- ME because SRES is not available to the ME.

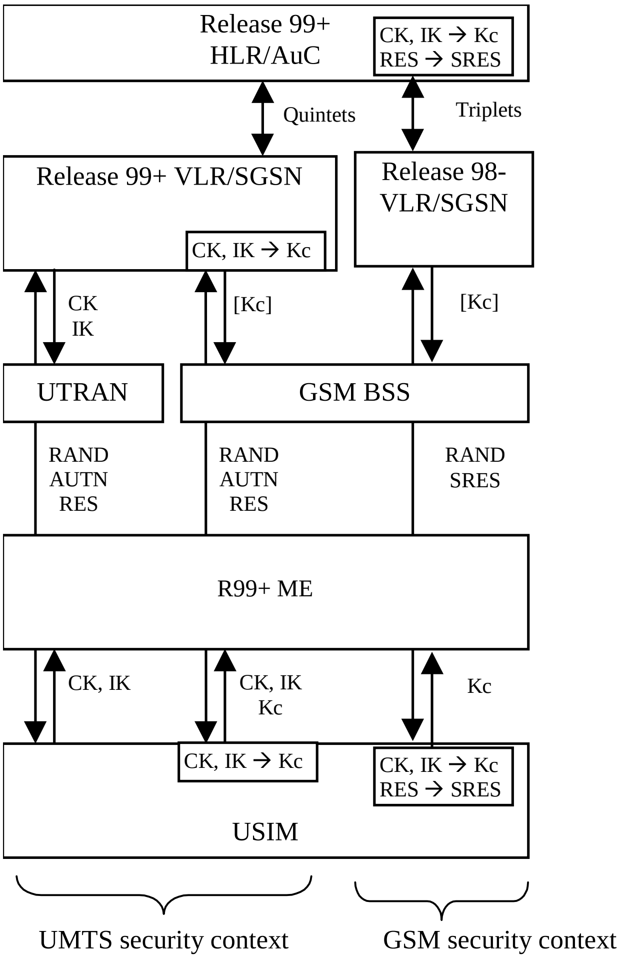


UMTS security context

3.4 USIM with functions c2 and c3

Changes from 33.102 V3.5.0:

- change UE to ME
- No conversion in the USIM for the left case (end to end 3G)
- A ME R98- does not support a USIM (removed)



4 Open questions

When the UICC contains a SIM and a USIM, the value IMSI and Ki should be shared for both contexts ?
UMTS IMSI is 64 bits
UMTS key K is 128 bits

We have the different possibilities:

1. $IMSI_{GSM}$ = $IMSG_{UMTS}$ and Ki_{GSM} = Ki_{UMTS}
2. $IMSI_{GSM}$ = $IMSG_{UMTS}$ and Ki_{GSM} != Ki_{UMTS}
3. $IMSI_{GSM}$!= $IMSG_{UMTS}$ and Ki_{GSM} = Ki_{UMTS}
4. $IMSI_{GSM}$!= $IMSG_{UMTS}$ and Ki_{GSM} != Ki_{UMTS}

Advantages:
$IMSI_{GSM}$!= $IMSG_{UMTS}$

The operator is able to differentiate the customer and apply different communication rate for the two contexts (GSM or UMTS)

Ki_{GSM} != Ki_{UMTS}

The security will be better. Even if the GSM key is found the UMTS security is still at the same level than before.

The decision could be left open and then be operator dependent.

5 Conclusion

This document should help to clarify the situations described in "6.8 Interoperation and handover between UMTS and GSM" of 33.102 V3.5.0

6 Annex

3G TS 31.102 V3.2.0 (2000-07) (Characteristics of the USIM Application) describes the AUTENTICATE USIM command.

7 USIM Commands

7.1 AUTHENTICATE

7.1.1 Command description

The function is used during the procedure for authenticating the USIM to its HE and vice versa. In addition, a cipher key and an integrity key are calculated. For the execution of the command the USIM uses the subscriber authentication key K, which is stored in the USIM.
The function is related to a particular USIM and shall not be executable unless the USIM or any sub-directory has been selected as the Current Directory and a successful PIN verification procedure has been performed (see clause 5).
The function can be used in two different contexts:

- a 3G security context, when 3G authentication vectors (RAND, CK, IK, AUTN) are available (i.e. the UE is located in the UTRAN, or in a GSM radio access network which is connected to a 3G or 3G capable MSC/VLR or SGSN), or

- a GSM security context, when GSM authentication data are available only (i.e. the UE is located in the GSM radio access network which is connected to a non-3G capable MSC/VLR or SGSN).

7.1.1.1 3G security context

The USIM first computes the anonymity key AK = $f5_K$ (RAND) and retrieves the sequence number SQN = (SQN ⊕ AK) ⊕ AK.
Then the USIM computes XMAC = $f1_K$ (SQN || RAND || AMF) and compares this with the MAC which is included in AUTN. If they are different, the USIM abandons the function.
Next the USIM verifies that the received sequence number SQN is in the correct range. This is described in annex C.If the USIM detects the sequence numbers to be not in the correct range, this is considered as a synchronisation failure and the USIM abandons the function. In

this case the command response is AUTS, where:

AUTS = Conc(SEQ_{MS}*) || MACS;*

Conc(SEQ_{MS}*) =* $SEQ_{MS} \oplus f5_K$*(MACS)* is the concealed value of the counter SEQ_{MS} in the USIM; and.

MACS = $f1*_K$*(*SEQ_{MS} || *RAND* || *AMF)* where:

RAND is the random value received in the current user authentication request;

the AMF assumes a dummy value of all zeroes so that it does not need to be transmitted in clear in the resynchronisation message.

If the sequence number is considered in the correct range, the USIM computes RES = $f2_K$ (RAND), the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND) and includes these in the command response. Note that if this is more efficient, RES, CK and IK could also be computed earlier at any time after receiving RAND.

The use of AMF is HE specific and while processing the command, the content of the AMF has to be interpreted in the appropriate manner. The AMF may e.g. be used for support of multiple algorithms or keys or for changing the size of lists, see 3G TS 33.102 [13].

If Service n°27 is "available", the USIM calculates the GSM response parameter K_C, using the conversion function defined in 3G TS 33.102 [13].

Input:

- RAND, AUTN (AUTN := SQN ⊕ AK || AMF || MAC).

Output:

- RES, CK, IK if Service n°27 is "not available".

or

- RES, CK, IK, K_C if Service n°27 is "available".

or

- AUTS.

7.1.1.2 GSM security context

USIM operation in an GSM security context is supported if Service n°38 is "available".

The USIM computes RES = $f2_K$ (RAND), the cipher key CK = $f3_K$ (RAND) and the integrity key IK = $f4_K$ (RAND). Next the USIM calculates the GSM response parameters SRES and K_C, using the conversion functions defined in 3G TS 33.102 [13].

Input:

- RAND.

Output:

- SRES; K_C.

7.1.2 Command parameters and data

Code	Value
CLA	As specified in 3G TS 31.101
INS	'88'
P1	'00'
P2	See table below
Lc	See below
Data	See below
Le	See below

Parameter P2 specifies the authentication context as follows:

Coding of the reference control P2

Coding b8-b1	Meaning
'1-------'	Specific reference data (e.g. DF specific/application dependant key)
'-XXXXXX-'	'000000'
'-------X'	Authentication context: 0 GSM context 1 3G context

All other codings are RFU.
Command parameters/data:

Byte(s)	Description	Length
1	Length of RAND (L1)	1
2 to (L1+1)	RAND	L1
(L1+2)	Length of AUTN (L2) (see note)	1
(L1+3) to (L1+L2+2)	AUTN (see note)	L2
Note: Parameter present if and only if in 3G security context.		

The coding of AUTN is described in 3G TS 33.102 [13]. The most significant bit of RAND is coded on bit 8 of byte 2. The most significant bit of AUTN is coded on bit 8 of byte (L1+3).
Response parameters/data, case 1, 3G security context, command successful:

Byte(s)	Description	Length
1	"Successful 3G authentication" tag = 'DB'	1
2	Length of RES (L3)	1
3 to (L3+2)	RES	L3
(L3+3)	Length of CK (L4)	1
(L3+4) to (L3+L4+3)	CK	L4
(L3+L4+4)	Length of IK (L5)	1
(L3+L4+5) to (L3+L4+L5+4)	IK	L5
(L3+L4+L5+5)	Length of K_C (= 8) (see note)	1
(L3+L4+L5+6 to (L3+L4+L5+13)	K_C (see note)	8
Note: Parameter present if and only if Service n°27 is "available".		

The most significant bit of RES is coded on bit 8 of byte 3. The most significant bit of CK is coded on bit 8 of byte (L3+4). The most significant bit of IK is coded on bit 8 of byte (L3+L4+5).

Response parameters/data, case 2, 3G security context, synchronisation failure:

Byte(s)	Description	Length
1	"Synchronisation failure" tag = 'DC'	1
2	Length of AUTS (L1)	1
3 to (L1+2)	AUTS	L1

The coding of AUTS is described in 3G TS 33.102 [13]. The most significant bit of AUTS is coded on bit 8 of byte 3.

Response parameters/data, case 3, GSM security context, command successful:

Byte(s)	Description	Length
1	Length of SRES (= 4)	1
2 to 5	SRES	4
6	Length of K_C (= 8)	1
7 to 14	K_C	8

The most significant bit of SRES is coded on bit 8 of byte 2. The most significant bit of Kc is coded on bit 8 of byte 7.