TSGS#24(04)0371

Source: **SA WG3 (Security)**

Title: **2 CRs to 33.105: Correction of inconsistencies in AK computation for re-synchronisation (Rel-4)**

Document for: **Approval**

Agenda Item: **7.3.3**

SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Workitem
S3-040371	33.105	021	-	Rel-4	Correction of inconsistencies in AK computation for re-synchronisation	F	4.1.0	S3-040402	SEC1

3GPP TSG SA WG3 Security — SA3#33 **S3-040402**
10-14 May 2004, Beijing, China

CR-Form-v7

CHANGE REQUEST

⌘ **33.105** **CR** **021** ⌘ **rev** **-** ⌘ Current version: **4.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [ ] Radio Access Network [ ] Core Network [X]

Title:	⌘	Correction of inconsistencies in AK computation for re-synchronisation
Source:	⌘	SA WG3
Work item code:	⌘	SEC1
Date:	⌘	23/04/2004
Category:	⌘	**F**
Release:	⌘	*Rel-4*

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*

Reason for change:	⌘	f5 is used instead of f5* in figures 3 and 4 to align the figures with the text.
Summary of change:	⌘	f5 is replaced by f5* in figures 3 and 4 to align the figures with the text.
Consequences if not approved:	⌘	Consistency problem. Potential misinterpretation of AK computation for re-synchronisation.

Clauses affected:	⌘	5.1.1.3, 5.1.1.4

Other specs affected: ⌘	Y	N		⌘
		X	Other core specifications	
		X	Test specifications	
		X	O&M Specifications	

Other comments: ⌘

********** BEGIN OF CHANGE **********

5.1.1.3 Generation of re-synchronisation token in the USIM

Upon the assertion of a synchronisation failure, the USIM generates a re-synchronisation token as follows:

a) The USIM computes MAC-S = $f1^*_K(SQN_{MS} \| RAND \| AMF^*)$, whereby AMF* is a default value for AMF used in re-synchronisation.

b) If SQN_{MS} is to be concealed with an anonymity key AK, the USIM computes $AK = f5^*_K(RAND)$, and the concealed counter value is then computed as $SQN_{MS} \oplus AK$.

c) The re-synchronisation token is constructed as $AUTS = SQN_{MS} [\oplus AK] \| MAC\text{-}S$.

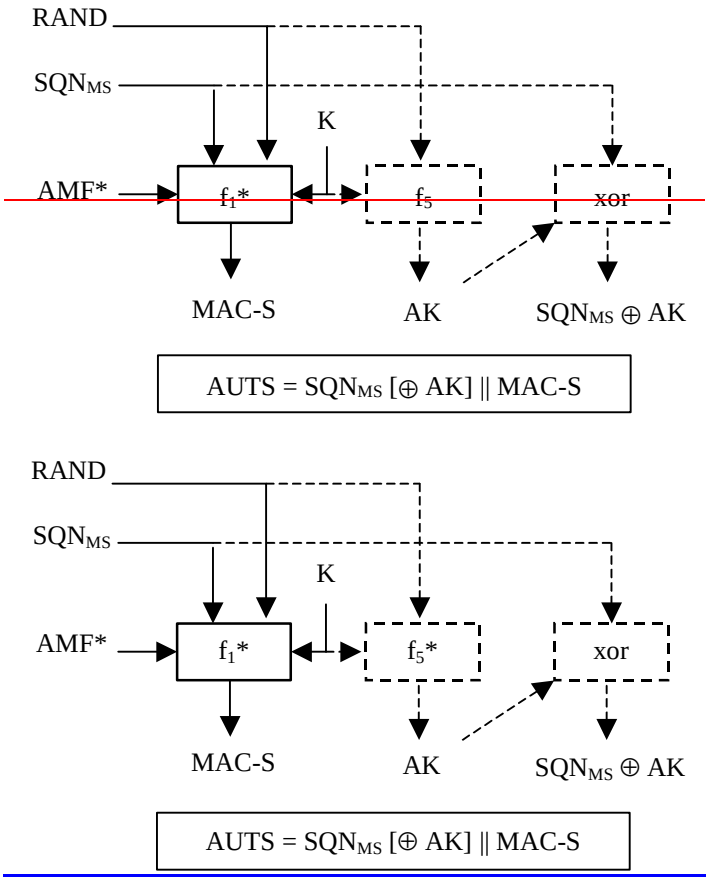

Figure 3: Generation of re-synchronisation token in the USIM

5.1.1.4 Re-synchronisation in the HLR/AuC

Upon receipt of an indication of synchronisation failure and a (AUTS, RAND) pair, the HLR/AuC may perform the following cryptographic functions:

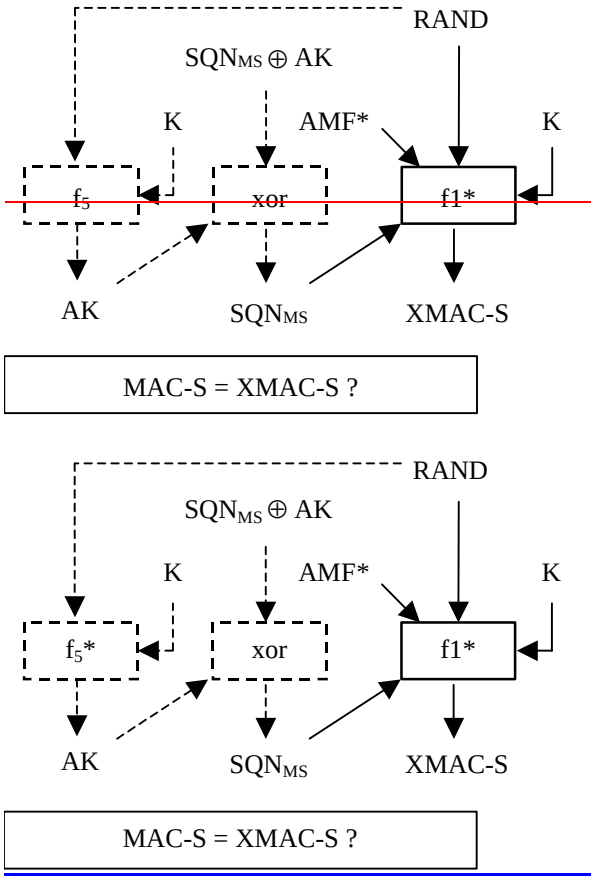

Figure 4: Re-synchronisation in the HLR/AuC

a) If SQN_{MS} is concealed with an anonymity key AK, the HLR/AuC computes AK = $f5^*_K$(RAND)and retrieves the unconcealed counter value as SQN_{MS} = (SQN_{MS} ⊕ AK) xor AK.

b) If SQN generated from SQN_{HE} would not be acceptable, then the HLR/AuC computes XMAC-S = $f1^*_K$(SQN_{MS} || RAND || AMF*), whereby AMF* is a default value for AMF used in re-synchronisation.

********** END OF CHANGE **********