3GPP TSG SA WG3 Security — S3#24 S3-020370

9 – 12 July 2002, Helsinki, Finland

CR-Form-v5

CHANGE REQUEST

⌘ **33.203** **CR** ⌘ **rev** **-** ⌘ Current version: **5.2.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Correcting the network behaviour in response to an incorrect AUT-S
Source:	⌘	Hutchison 3G UK
Work item code:	⌘	***Date:*** ⌘ 4/7/02
Category:	⌘ **F**	***Release:*** ⌘ Rel-5

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)*

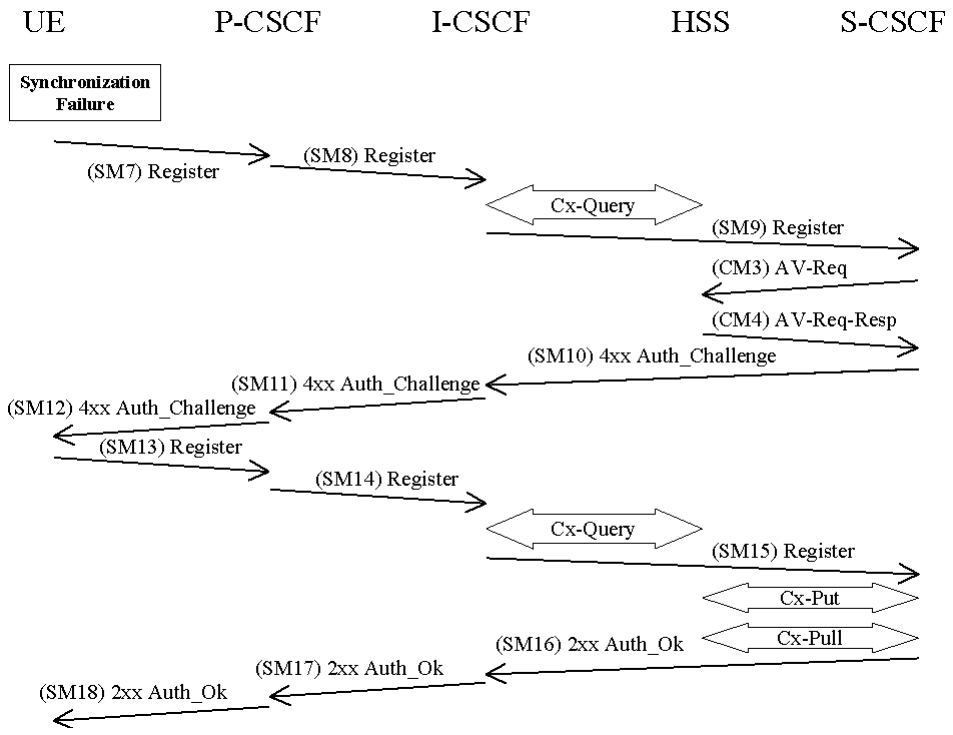
Reason for change:	⌘	Currently the text states the behaviour should follow the behaviour in TS 33.102. It also makes returning AVs conditional on a successful checking of AUTS. This is out of line with TS 33.102 which returns AVs regardless of whether AUTS was successful or not. The change is to make the behaviour describe inline with TS 33.102
Summary of change:	⌘	To make the HSS always return AVs whether the AUTS check is successful or not.
Consequences if not approved:	⌘	Inconsistency in the specification that could lead to incompatible implementations.

Clauses affected:	⌘	6.1.3		
Other specs affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	
Other comments:	⌘			

6.1.3 Synchronization failure

~~[Editor's note: This subsection shall deal with the requirements for the case when the SQNs in the ISIM and the HSS are not in synch.]~~

In this section the case of an authenticated registration with synchronization failure is described. After re-synchronization, authentication may be successfully completed, but it may also happen that in subsequent attempts other failure conditions (i.e. user authentication failure, network authentication failure) occur. In below only the case of synchronization failure with subsequent successful authentication is shown. The other cases can be derived by combination with the flows for the other failure conditions.



The flow equals the flow in 6.1.1 up to SM6. When the UE receives SM6 it detects that the SQN is out of range and sends a synchronization failure back to the S-CSCF in SM7. Draft-ietf-sip-digest-aka-01 [17] describes the fields to populate corresponding parameters of synchronization failure.

SM7:
REGISTER(Failure = *Synchronization Failure,* AUTS, IMPI*)*

Upon receiving the *Synchronization Failure* and the AUTS the S-CSCF sends an Av-Req to the HSS in CM3 including the required number of Avs, n.

CM3:
Cx-AV-Req(IMPI, RAND,AUTS, n)

The HSS checks the AUTS as in section 6.3.5 in [1]. ~~If the check is successful and~~ After potentially ~~after~~ updating the SQN, the HSS ~~creates and~~ sends new AVs to the S-CSCF in CM4.

CM4:
Cx-AV-Req-Resp(IMPI, n,$RAND_1$||$AUTN_1$||$XRES_1$||CK_1||IK_1,….,$RAND_n$||$AUTN_n$||$XRES_n$||CK_n||IK_n)

The rest of the messages i.e. SM10-SM18 including the Cx messages are exactly the same as SM4-SM12 and the corresponding Cx messages in 6.1.1.