3GPP TSG-SA3 Meeting #34
Acapulco, Mexico, 6-9 July 2004

Tdoc ⌘S3-040634

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **5.8.0** ⌘

*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⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Deletion of old authentication vectors in S-CSCF after re-synchronization
Source:	⌘	Nokia
Work item code:	⌘	IMS-ASEC
Date:	⌘	23/06/2004
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)*
Rel-6	*(Release 6)*

Reason for change:	⌘	It is not described in the TS 33.203 that S-CSCF must delete those authentication vectors it has in storage and which it has received from the HSS before the re-synchronization was performed.
Summary of change:	⌘	S-CSCF deletes old authentication vectors when it receives the new batch of authentication vectors from the HSS as an response to the authentication vector request with re-synchronization indication.
Consequences if not approved:	⌘	If S-CSCF doesn't delete the old authentication vectors it has in storage, new re-synchronization errors will occur.

Clauses affected:	⌘	6.1.3

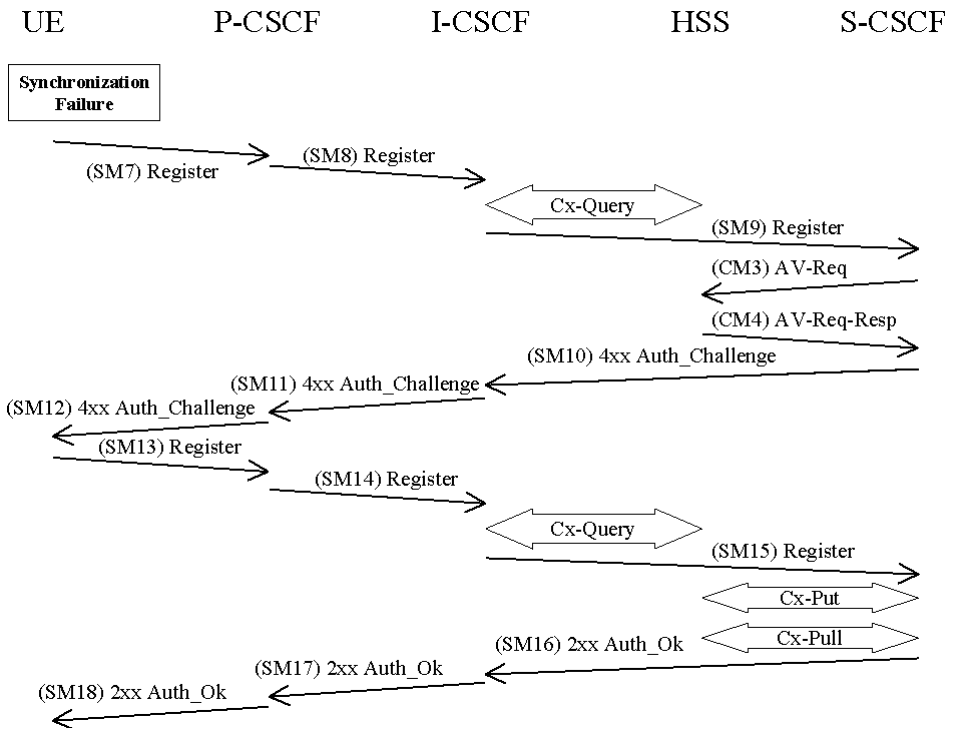
Other specs affected: ⌘	Y	N		⌘	
	X		Other core specifications	⌘	24.229
		X	Test specifications		
		X	O&M Specifications		

Other comments:	⌘	

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

6.1.3 Synchronization failure

In this clause 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. RFC 3310 [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 RAND stored by the S-CSCF and the required number of Avs, m.

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

The HSS checks the AUTS as in clause 6.3.5 of TS 33.102 [1]. After potentially updating the SQN, the HSS 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)

When the S-CSCF receives the new batch of authentication vectors from the HSS it deletes the old ones for that user in the S-CSCF.

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.

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