3GPP TSG SA WG3 Security — S3#23 S3-020208

14 - 17 May 2002

Victoria, Canada

CR-Form-v5

CHANGE REQUEST

⌘ **TS33.203** **CR** ⌘ **rev** **-** ⌘ Current version: **5.1.0** ⌘

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

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

Title:	⌘	Correction to S-CSCF behaviour on Network Authentication Failure
Source:	⌘	Hutchison 3G UK
Work item code:	⌘	***Date:*** ⌘ 09/05/02
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.

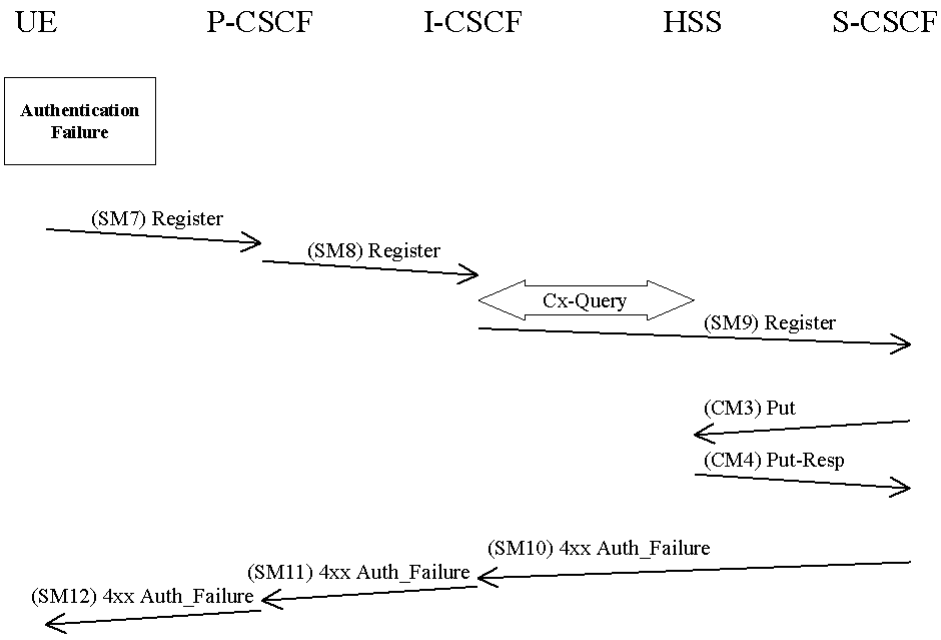
Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	Currently the S-CSCF de-registers the user on network authentication failure. This is not the desired behaviour as it allows an attacker to de-register a subscriber.
Summary of change:	⌘	The S-CSCF does not de-register the IMPU on network authentication failure if the IMPU is already registered.
Consequences if not approved:	⌘	An attacker could force an IMPU to be de-registered.

Clauses affected:	⌘	6.1.2.2
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

6.1.2.2 Network authentication failure

In this section the case when the authentication of the network is not successful is specified. When the check of the MAC in the UE fails the network can not be authenticated and hence registration fails. The flow is identical as for the successful registration in 6.1.1 up to SM6.



The UE shall send a Register message towards the HN including an indication of the cause of failure in SM7. The P-CSCF and the I-CSCF forward this message to the S-CSCF.

SM7:
REGISTER(Failure = *AuthenticationFailure*, IMPI)

Upon receiving SM9, which includes the cause of authentication failure, the S-CSCF shall set the registration-flag to *unregistered*, if the IMPU is not already registered. If the IMPU was already registered, the S-CSCF does not update the registration flag. To set the flag the S-CSCF sends in CM3 a Cx-Put ~~in CM3~~ to the HSS.~~and receives a Cx-Put-Resp in CM4.~~

CM3:
Cx-AV-Put(IMPI, IMPU, Clear S-CSCF name)

~~The S-CSCF sends a Cx-Put (CM3) to the HSS, which indicates that authentication failed and that, the S-CSCF should be cleared.~~ The HSS responds with a Cx-Put-Resp in CM4.

In SM10 the S-CSCF sends a 4xx Auth_Failure towards the UE indicating that authentication has failed, no security parameters shall be included in this message.

SM10:
SIP/2.0 4xx Auth_Failure

Upon receiving SM10 the I-CSCF shall clear any registration information related to the IMPI.

~~[Editor's note: It is FFS if same header i.e. 4xx Auth_Failure shall be used for both UE and network authentication failure.]~~