3GPP TSG-SA-WG3 Meeting #31
18th – 21st November 2003, Munich, Germay

Tdoc ⌘S3-030770

CR-Form-v7

CHANGE REQUEST

⌘	**TS 33.203**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	**5.7.0** ⌘

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:	⌘	Network behaviour when a new REGISTER is challenged during an on going authentication			
Source:	⌘	**Nokia, 3**			
Work item code:	⌘	IMS-ASEC	***Date:***	⌘	19/11/2003
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 was agreed in the SA3/CN1 joint meeting that the S-CSCF may challenge a UE when it already has an authentication running with that UE, but the CSCFs should have only one authentication running with a particular UE. This CR is an implementation of that conclusion.

Summary of change: ⌘ When the S-CSCF challenges a new REGISTER while still waiting for a response to a previous challenge then

- The S-CSCF should abandon the previous challenge,
- The P-CSCF should delete the previous registration SA to the same UE, and insert the one that is associated with new challenge.

Consequences if not approved: ⌘ Not allowing the S-CSCF to start a new authentication and abandon the previous authentication (before it has timed out) severely increases the ability of an attacker to prevent a genuine UE from registering with the network.

Clauses affected: ⌘ 6.1.2.3, 7.3.1.4

		Y	**N**			
Other specs affected:	⌘	**X**		Other core specifications	⌘	TS 24.229, TS 29.228
			X	Test specifications		
			X	O&M Specifications		

Other comments: ⌘

6.1.2.3 Incomplete authentication

When the S-CSCF receives a new REGISTER request and challenges this request, it considers any previous authentication to have failed. It shall delete any information relating to the previous authentication, although the S-CSCF may send a response if the previous challenge is answered. A challenge to the new request proceeds as described in clause 6.1.1.

If the S-CSCF does not receive a response to an authentication within an acceptable time, it considers the authentication to have failed. If the IMPU was not already registered, the S-CSCF shall send a Cx-Put to the HSS to set the registration-flag for that IMPU to unregistered (see message CM3 in clause 6.1.2.2). If the IMPU was already registered, the S-CSCF does not change the registration-flag.

------ NEXT CHANGE------

7.3.1.4 Incomplete authentication

If the UE responds to an authentication challenge from a S-CSCF, but does not receive a reply before the request times out, the UE shall start a registration procedure if it still requires any IM services. The first message in this registration should be protected with an SA created by a previous successful authentication if one exists.

When the P-CSCF receives a challenge from the S-CSCF and creates the corresponding SAs during a registration procedure, it shall delete any information relating to any previous registration procedure (including the SAs created during the previous registration procedure).

If the P-CSCF deletes a registration SA due to its lifetime being exceeded, the P-CSCF should delete any information relating to ~~that~~ the registration procedure that created the SA.